Residential Gateway

Contents

1 INTRODUCTIONS 4

1.1 APPLICATIONS 4
1.2 FEATURES 4
1.3 WIRELESS SPEC 4
1.4 COMPLIANCE CERTIFICATES 5
1.5 STANDARDS COMPATIBILITY AND COMPLIANCE 5
1.6 ENCAPSULATION SUPPORTS 6
1.7 ENVIRONMENT 6
1.8 SYSTEM REQUIREMENTS 6
1.9 SAFETY CAUTIONS 8
1.10 LED STATUS DESCRIPTION 8
1.10.1 LED Status Description 8
1.10.2 Rear panel 9

2 HARDWARE INSTALLATION 9

2.1 CHOOSING THE BEST LOCATION FOR WIRELESS OPERATION 9
2.2 ADSL ROUTER'S CONNECTION 10
2.3 FACTORY RESET BUTTON 10
2.4 USB INSTALLATION 10

3 INTRODUCTION 13

3.1 ABOUT DSL ROUTER 13
3.2 SETUP 13
3.2.1 Setting up WAN and LAN connections 14
3.2.2 PC Network Configuration 14

4 WEB-BASED MANAGEMENT 15

4.1 LOGGING ON THE MODEM 15
4.1.1 First Time Logging 15
4.2 QUICK SETUP 16
4.2.1 WAN Interface Setup 16
4.2.2 LAN Inerface Setup 26
4.2.3 Wireless Interface Setup 27
4.2.4 WAN Setup Summary 27
4.2.5 Quick Setup Completed 28
4.3 DSL ROUTER DEVICE INFORMATION 29
4.3.1 Summary of Device information 29
4.3.2 WAN Interface information 30
4.3.3 Statistics 31
4.3.4 Statistics of LAN 31
4.3.5 Statistics of WAN 31
4.3.6 Statistics of ATM 32
4.3.7 Statistics of ADSL 33
4.3.8 Route table information 35
4.3.9 ARP table information 35
4.3.10 DHCP IP Leases information 36
4.4 ADVANCED SETUP 36
4.4.1 WAN CONFIGRATION 37
4.4.2 LAN configuration 63
4.4.3 NAT-- Network Address Translation 67
4.4.4 Security 72
4.4.5 Quality of Service 80
4.4.6 Routing 87
4.4.7 DNS 94
4.4.8 DSL 96
4.4.9 Print Server 97

4.4.10 Port Mapping 101
4.4.11 IPsec 102
4.4.12 Certificate 106
4.5 WIRELESS 109
4.5.1 Overview 109
4.5.2 Wireless LAN Basics 111
4.5.3 Configure Wireless Connection 115
4.5.4 Configuration Example 131
4.6 VOICE (AVAILABLE) 133
4.6.1 Overview 133
4.6.2 Web Page Introduction 138
4.6.3 VoIP functionality 144
4.6.4 Configuration Example 148
4.7 USB STORAGE 151
4.7.1 FTP Server Configure 152
4.8 DIAGNOSTICS 153
4.9 MANAGEMENT 154
4.9.1 Settings 154
4.9.2 System Log 154
4.9.3 SNMP Client 156
4.9.4 TR-69 Client Management 162
4.9.5 Internet Time 164
4.9.6 Access Control 164
4.9.7 Update Software 166
4.9.8 Save/Reboot 166

1 Introductions

The DSL Router is a Highly integrated ADSL2+ Integrated Access Device , which is an advanced all-in-one gateways incorporating VoIP(available), Ethernet Switch, and Wireless home networking Access Point ,complied with the IEEE802.11b/g standards. It is usually prefered to provide high access performance applications for the individual users,the SOHO,the small enterprise and so on.

1.1 Applications

- Home gateway
- SOHO Applications
- The small enterprise Appllications
- Voice over IP(available)
- TV over IP (IPTV)
- Higher data rate broadband sharing
- Shared broadband internet access
- Audio and video streaming and transfer
- PC file and application sharing
- Network and online gaming

1.2 Features

- Four 10/100 Ethernet ports
- 1x USB 2.0 host port
- Friendly GUI for web configuration.
- Support IPSec for Virtual Private Network (VPN)
- Several popular games are already pre-configured. Just enable the game and the port settings are automatically configured.
- Configurable as a DHCP Server on Your Network
- Compatible with virtually all standard Internet applications
- Industry standard and interoperable DSL interface
- Support Virtual Server, IP Filter, DMZ Host, and Much More
- Simple web based status page displays a snapshot of system configuration, and links to the configuration pages
- Downloadable flash software upgrades
- Support for up to 16 Permanent Virtual Circuits (PVC)
- Support for up to 8 PPPOE sessions
- Support SNMP v2, RIP v1 & RIP v2 , NAT
- WLAN with High-Speed Data Transfer Rates of up to 54Mbps, Compatible with IEEE 802.11b/g, 2.4GHz Compliant Equipment

1.3 Wireless Spec

Network Standard		IEEE 802.11b IEEE 802.11g
Frequency Range		2.40G-2.4835Ghz ISM Band
Modulation		802.11b： DBPSK、DQPSK、 CCK 802.11g： BPSK、QPSK、16QAM、64QAM
RF Power		20dBm(Max). Typ. 18 dBm @Normal Temp Range; 802.11g: Typ. 15 dBm @ Normal Temp Range
AP Capacity	Access User Quantity	50～80Pcs/AP (Proposal)

	Channels	11 (US and Canada) 13 (Europe and China) 14 (Japan)
	Auto-sensing Data Rate	1Mbps、2Mbps、5.5Mbps、11Mbps for 802.11.b
		6 Mbps、9 Mbps、12 Mbps、18 Mbps、24 Mbps、36 Mbps、48 Mbps、54 Mbps for 802.11b
Payload Rate	1Mbps	DBPSK @ 0.81Mbps
	2Mbps	DQPSK @ 1.58Mbps
	5.5Mbps	CCK @ 4.07Mbps
	6 Mbps	BPSK@4.64Mbps
	9 Mbps	BPSK@6.55Mbps
	11 Mbps	CCK @ 7.18Mbps
	12 Mbps	BPSK @8.31 Mbps
	18 Mbps	QPSK@11.5 Mbps
	24 Mbps	6QAM@14.18 Mbps
	36 Mbps	16QAM@18.31 Mbps
	48 Mbps	64QAM@23.25 Mbps
	54 Mbps	64QAM @26.12 Mbps
Security		64-bit/128-bit WEP, 802.1x, WPA, WPA2
User Isolation		MAC Level
MAC Filter	Eth Interface MAC Filter	Support
	Vacancy MAC Filter	Support
Authentication	DHCP Client & Static IP	Support
	802.1X and Radius Client	Support
	DHCP Server	Support
Radio Cover Rage (m)	Outdoor	120～400
	Indoor	35～100
Antenna Type	Internal Diversity with Connector. 2dBi	

1.4 Compliance Certificates

- FCC Class B
- CE Mark

1.5 Standards Compatibility and Compliance

- RFC 2684 multiprotocol Encapsulation over ATM Adaptation Layer 5
- RFC1483 Multiprotocol Encapsulation over ATM Adaptation Layer 5
- RFC2364 PPP over ATM ALL5(PPPoA)
- RFC2516 PPP Over Ethernet (PPPoE)
- RFC1662 PPP in HDLC-like Framing
- RFC1332 PPP Internet Protocol Control Protocol
- RFC1577/2225 Classical IP and ARP over ATM(IPoA)
- RFC1483R
- RFC894 A Standard for the Transmission of IP Datagrams over Ethernet Networks
- RFC1042 A standard for the Transmission of IP Datagrams over IEEE 802 Networks
- MER(a.k.a IP over Ethernet over AAL5)
- Support ALG(Application Level Gateways)
- ITU G.992.1 (G.dmt)
- ITU G.992.2 (G.lite)
- ITU G.994.1 (G.hs)
- ITU G.992.3 (ADSL2)
- ITU G.992.5 (ADSL2+)

- ANSI T1.413 issue 2
- IEEE802.3
- IEEE802.3u
- IEEE 802.11b
- IEEE 802.11g
- RFC3261(SIP for VoIP)

1.6 Encapsulation Supports

- RFC 1483 bridge
- RFC 1483 Router
- Classical IP over ATM (RFC 1577)
- PPP over ATM (RFC 2364)
- PPP over Ethernet (RFC 2516)

1.7 Environment

- Operating temperature: 0℃ to 40℃(32ºF to 104ºF)
- Storage temperature: -20℃ to 70℃(-4ºF to 158ºF)
- Operating Humidity: 10%~95% no freezing
- Storage humidity: 5%~95% no freezing

1.8 System requirements

Recommended system requirements are:
- Pentium 233MHZ or above
- Memory: 64MB or above
- 10M Base-T Ethernet or above
- WIN9X, WIN2000, WINXP, WINME, WINNT
- Ethernet Network Interface Card

Please collect the following information. This information will be very helpful for your ADSL configuration. To keep a record for reference, you can fill in the column as below.

Information you will need from your ADSL service provider:

VPI	Most users will not be required to change this setting. The Virtual Path Identifier (VPI) is used in conjunction with the Virtual Channel Identifier (VCI) to identify the data path between your ADSL service provider's network and your computer. If you are setting up the Router for multiple virtual connections, you will need to configure the VPI and VCI as instructed by your ADSL service provider for the additional connections. This setting can be changed in the WAN menu of the web management interface.	Record info here
VCI	Most users will not be required to change this setting. The Virtual Channel Identifier (VCI) used in conjunction with the VPI to identify the data path between your ADSL service provider's network and your computer. If you are setting up the Router for multiple virtual connections, you will need to configure the VPI and VCI as instructed by your ADSL service provider for the additional connections. This setting can be changed in the WAN menu of the web management interface.	
Connection and Encapsulation Type	This is the method your ADSL service provider uses to transport data between the Internet and your	

	computer. Most users will use the default PPPoE/PPPoA, connection type. The Setup Wizard can be used to configure a PPPoE/PPPoA connection type. You may need to specify one of the following connection types (PPPoE LLC, PPPoA LLC or PPPoA VC-MUX). The other available connection and encapsulation combinations must be configured using the web manager. These include Bridge Mode (1483 Bridged IP LLC or 1483 Bridged IP VC-MUX), and Static IP (Bridged IP LLC, 1483 Bridged IP VC-MUX, 1483 Routed IP LLC, 1483 Routed IP VC-MUX or IPoA) etc.	
Username	This is the Username used to log on to your ADSL service provider's network. It is commonly in the form: user@isp.com. Your ADSL service provider uses this to identify your account.	
Password	This is the Password used, in conjunction with the Username above, to log on to your ADSL service provider's network. This is used to verify the identity of your account.	

Information you will need about your DSL Router Residential Gateway:

LAN IP addresses for the DSL Router	This is the IP address you will enter into the Address field of your web browser to access the gateway's configuration graphical user interface (GUI) using a web browser. The default IP address is **192.168.1.1** and it is referred to as the "Management IP" address in this User's Manual. This may be changed to suit any IP address scheme the user desires. This address will be the base IP address used for DHCP service on the LAN when DHCP is enabled.	Record info here
LAN Subnet Mask for the DSL Router	This is the subnet mask used by the DSL Router, and will be used throughout your LAN. The default subnet mask is **255.255.255.0**. This can be changed later.	
Username	This is the Username needed access the gateway's management interface. When you attempt to connect to the device through a web browser you will be prompted to enter this Username. The default Username for the Router is **admin**. The user cannot change this.	
Password	This is the Password you will be prompted to enter when you access the gateway's management interface. The default Password is **admin**. The user may change this.	

Information you will need about your LAN or computer:

Ethernet NIC	If your computer has an Ethernet NIC, you can connect the DSL Router to this Ethernet port using an Ethernet cable. You can also use the Ethernet ports on the DSL Router to connect to other computer or Ethernet devices.	Record info here
DHCP Client status	Your DSL Router Residential Gateway is configured, by default, to be a DHCP server. This means that it can assign an IP address, subnet mask, and a default gateway address to computers on your LAN. The default range of IP addresses the DSL Router will assign are from **192.168.1.2** to **192.168.1.254**. Your computer (or computers) needs to be configured to **Obtain an IP address automatically** (that is, they need to be configured	

	as DHCP clients.)	

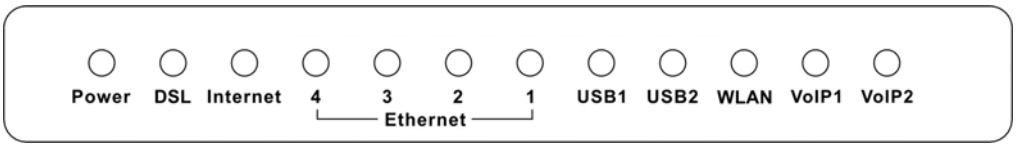
1.9 Safety Cautions

Follow these announcements below to protect the device from risks and damage caused by fire and electric power.

- Use volume labels to mark the type of power.
- Use the power adapter which is packed within the device package.
- Pay attention to the power load of the outlet or prolonged lines. A overburden power outlet or damaged lines and plugs may cause electric shock or fire accident. Check the power cords regularly. If you find any damage, replace it at once.
- Proper space left for heat radiation is necessary to avoid any damage caused by overheating to the device. The long and thin holes on the Access Point are designed for heat radiation to make sure the device works normally. Don't cover these heat radiant holes.
- Do not put this device close to a place where a heat source exits or high temperature occurs. Avoid the device from direct sunshine.
- Do not put this device close to a place where is over damp or watery. Do not spill any fluid on this device.
- Do not connect this device to any PC or electronic product, unless our customer engineer or your broadband provider instructs you to do this, because any wrong connection may cause any power or fire risk.
- Do not place this device on an unstable surface or support.

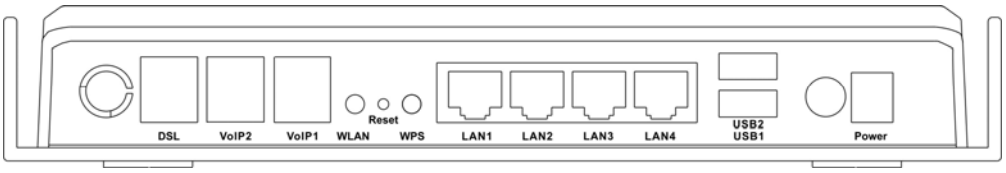
1.10 LED Status Description

1.10.1 LED Status Description



Indicator	Status	Description
POWER	Off	Power not supplied
	ON	Power supplied
WLAN	ON	WLAN link is established
	Blink	WLAN traffic is flowing
	Off	WLAN is disabled
Ethernet (1-4)	ON	ETH line is connected
	Blink	ETH traffic is flowing
	Off	ETH line is not connected
VoIP(available)	ON	VoIP Phone is registered
	Blink	Phone is off-hook
	Off	VoIP Phone is not registered
Internet	Blink	DSL traffic is flowing
DSL	Quick Blink	DSL line is training
	ON	DSL line is connected
	Off	DSL line is not connected

1.10.2 Rear panel



Interface	Description
SWITCH	Power on/off switch
Power Socket	Plug in for power adaptor
LAN	LAN interface for connecting to computer or Switch
USB host	Connect other USB device to supply some added value application
RESET	Modem Reset button Press to reset the hardware and the modem will auto restart. This action will recover the modem's default configuration.
WPS button	WLAN Security Easy Setup First short press to create a WPS network and WPS led is on; other short press enable WPS client to register and WPS led is blink; Long press(hold for 5sec) to disable this function when WPS led is on.
LINE	ADSL connector for connecting to ADSL telephone line

2 Hardware Installation

The DSL Router maintains three separate interfaces, an Ethernet LAN, a wireless LAN and an ADSL (WAN) interface. Place the Router in a location where it can be connected to the various devices as well as to a power source. The Router should not be located where it will be exposed to moisture or excessive heat. Make sure the cables and power cord are placed safely out of the way so they do not create a tripping hazard. As with any electrical appliance, observe common sense safety procedures. The Router can be placed on a shelf or desktop, ideally you should be able to see the LED indicators on the front if you need to view them for troubleshooting.

2.1 Choosing the Best Location for Wireless Operation

Many environmental factors can affect the effective wireless function of the DSL Router. If this is your first time setting up a wireless network device, read and consider the points listed below. The access point can be placed on a shelf or desktop, ideally you should be able to see the LED indicators on the front if you need to view them for troubleshooting.
Designed to go up to 100 meters indoors and up to 300 meters outdoors, Wireless LAN lets you access your network from anywhere you want. However, the number of walls, ceilings, or other objects that the wireless signals must pass through can limit signal range. Typical ranges vary depending on the types of materials and background RF noise in your home or business. For optimum range and signal strength, use these basic guidelines:

- **Keep the number of walls and ceilings to a minimum:**

The signal emitted from Wireless LAN devices can penetrate through ceilings and walls. However, each wall or ceiling can reduce the range of Wireless LAN devices from 1 to 30M. Position your wireless devices so that the number of walls or ceilings obstructing the signal path is minimized.

- **Consider the direct line between access points and workstations:**

A wall that is 0.5 meters thick, at a 45-degree angle appears to be almost 1 meter thick. At a 2-degree angle, it is over 14 meters thick. Be careful to position access points and client adapters so the signal can travel straight through (90º angle) a wall or ceiling for better reception.

- **Building Materials make a difference:**

Buildings constructed using metal framing or doors can reduce effective range of the device. If possible, position wireless devices so that their signal can pass through drywall or open doorways, avoid positioning them so that their signal must pass through metallic materials. Poured concrete walls are reinforced with steel while cinderblock walls generally have little or no structural steel.

- **Position the antenna for best reception:**

Play around with the antenna position to see if signal strength improves. Some adapters or access points allow the user to judge the strength of the signal.

- **Keep your product away (at least 1-2 meters) from electrical devices:**

Positions wireless devices away from electrical devices that generate RF noise such as microwave ovens, monitors, electric motors, etc.

2.2 ADSL Router's connection

- As illustrated below: Connect the DSL port of the DSL Router with telephone cable.
- Connect the LAN port of the DSL Router to the network card of the PC via a Ethernet line.
- Plug the power adapter to the wall outlet and then connect the other end of it to the PWR port of the DSL Router.

Connection 1: Fig. 2-1 displays the application diagram for the connection of the DSL Router, PC and telephones.

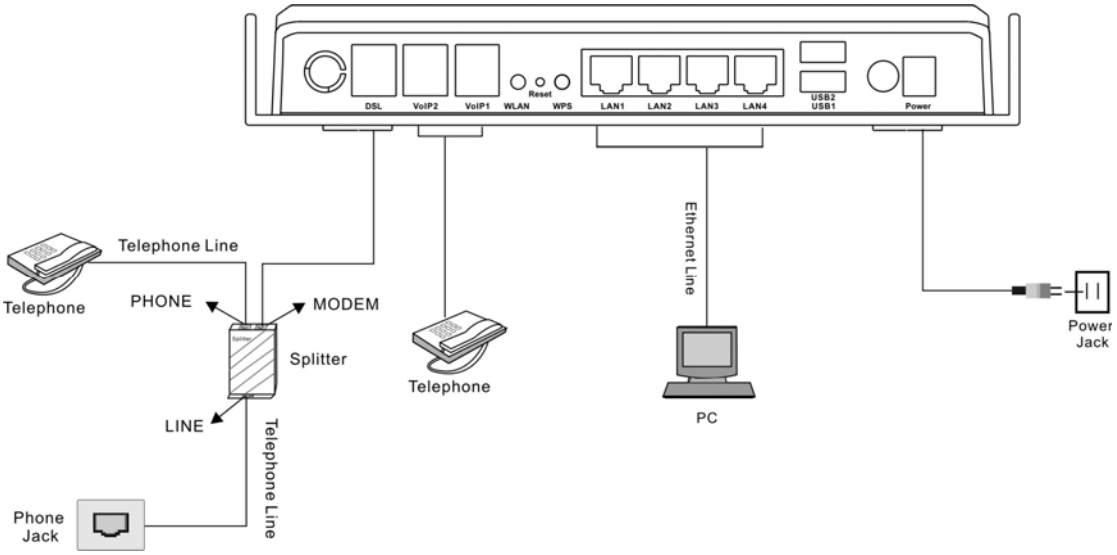


Fig. 2-1

2.3 Factory Reset Button

The Router may be reset to the original factory default settings by depressing the reset button for a few seconds while the device is powered on. Use a ballpoint or paperclip to gently push down the reset button. Remember that this will wipe out any settings stored in flash memory including user account information and LAN IP settings. The device settings will be restored to the factory default IP address 192.168.1.1 and the subnet mask is 255.255.255.0, the default management Username is admin and the default Password is admin.

2.4 USB Installation

To connect the DSL gateway to the PC's USB port, perform the following:

- Connect the USB cable to the USB port on the DSL gateway. The cable has two different

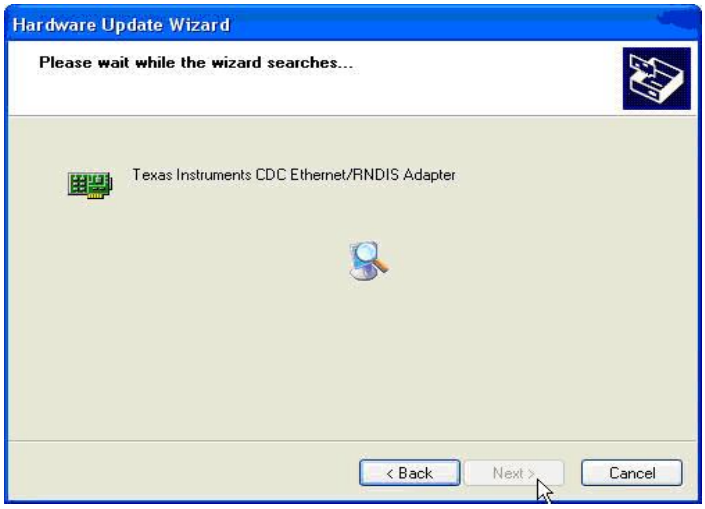
connectors; you may have to try both connectors and the connector is keyed so try different orientations.

- Connect the other end of the USB cable into the PC's USB port
- For the USB installation on Windows XP, once the PC powers up, a message tips shows Found new hardware on the system tray.

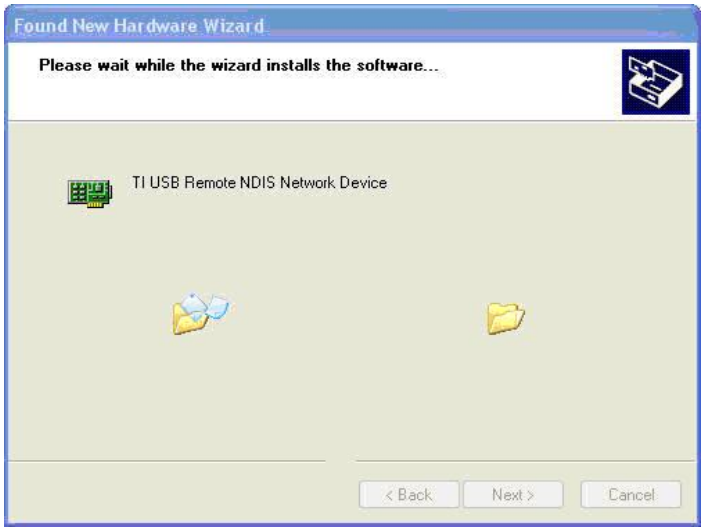
Then a dialog window Found New Hardware Wizard pop-up, Select Install the software automatically (Recommended) and insert the Manual and Driver CD-Rom. Click <Next >, the windows will search CD-Rom for the best USB driver.

Found New Hardware Wizard
Welcome to the Found New Hardware Wizard
This wizard helps you install software for:
Texas Instruments CDC Ethernet/RNDIS Adapter
If your hardware came with an installation CD or floppy disk, insert it now.
What do you want the wizard to do?
Install the software automatically (Recommended)
Install from a list or specific location (Advanced)
Click Next to continue.
< Back
Next >
Cancel

The dialog prompted Please wait while the wizard searches.



The USB driver has be searched by the Windows.



Ignore the windows warning for has not passed Windows Logo testing Windows XP, Click <Continue Anyway>.

Hardware Installation
The software you are installing for this hardware:
TI USB Remote NDIS Network Device
has not passed Windows Logo testing to verify its compatibility with Windows XP. (Tell me why this testing is important.)
Continuing your installation of this software may impair or destabilize the correct operation of your system either immediately or in the future. Microsoft strongly recommends that you stop this installation now and contact the hardware vendor for software that has passed Windows Logo testing.
Continue Anyway
STOP Installation

Click the button<Finish> to complete the USB driver installation.

Found New Hardware Wizard
Completing the Found New Hardware Wizard
The wizard has finished installing the software for:
TI USB Remote NDIS Network Device
Click Finish to close the wizard.
< Back
Finish
Cancel

3 Introduction

3.1 About DSL router

DSL router is a scalable suite of software infrastructure and technologies that Original Equipment Manufacturers (OEMs) require in order to bring Residential Gateways/Internet Access Devices (IADs) to market.
DSL router leverages a wide range of compelling broadband-based applications and services and includes an operating system, drivers and remote management capabilities. DSL router delivers a set of highly integrated solutions, required for the home and small of company, such as:
.Optimized Linux 2.6 Operating System
. IP Routing and Bridging
. Asynchronous Transfer Mode (ATM) and Digital Subscriber Line (DSL) support
. Point-to-Point Protocol (PPP)
. Network/Port Address Translation (NAT/PAT)
. Quality of Service (QoS)
. Wireless LAN Security: WPA, 802.1x, RADIUS client
. Virtual Private Network (VPN): IPSec
. Secure Socket Layer Virtual Private Network (SSL VPN)
. Universal Plug-and-Play
. File Server for Network Attached Storage (NAS) devices
. Print Server
. Web Filtering
. Carrier Grade Voice over IP (VoIP): SIP, MGCP, RTP
. Management and Control: Web-based Management (WBM), Simple Network Management Protocol(SNMP), Command Line Interface (CLI), TR-069WAN Management Protocol, TR-064-LAN-Side DSL CPE Configuration.
. Remote Update
. System Statistics and Monitoring
. DSL router is targeted at the following platforms: DSL modems, Wireless access points and bridge.

3.2 Setup

Connecting your computer or home network to the DSL router is a simple procedure, varying slightly depending on your operating system. This chapter will help you to seamlessly integrate DSL router with your computer or home network. The Windows default network settings dictate that in most cases the setup procedure described below will be unnecessary. For example, the default DHCP setting in Windows 2000 is 'client', requiring no further modification. However, it is advised to follow the setup procedure described below to verify that all communication parameters are valid and that the physical cable connections are correct.The setup procedure consists of three consecutive configuration stages:

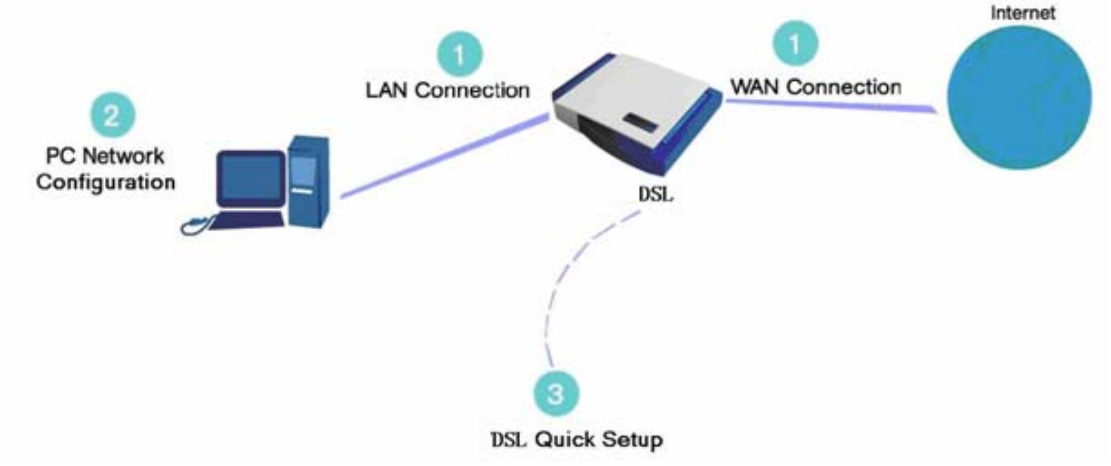


Figure 1.1: Hardware Configuration

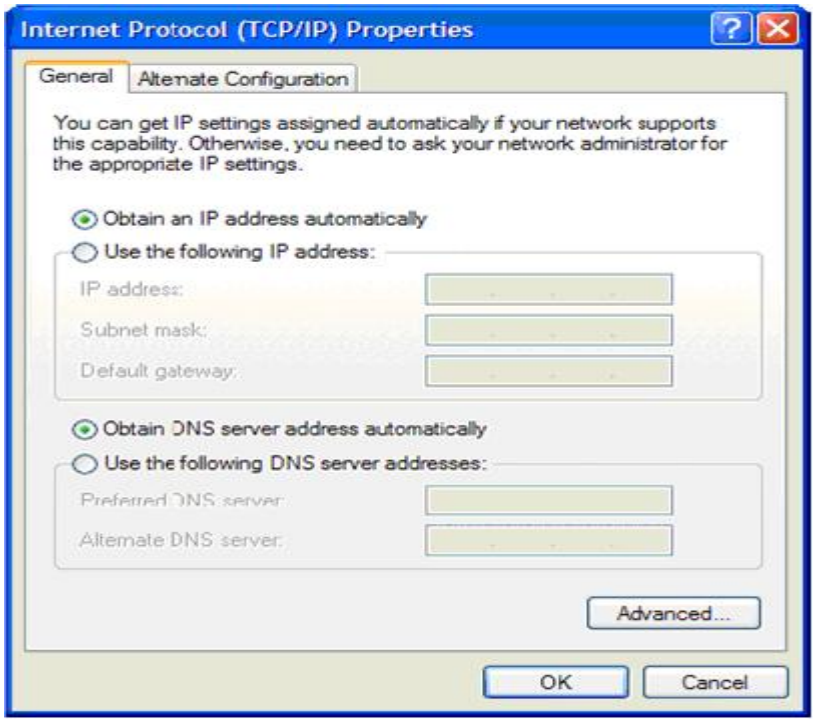
a. Setting up WAN and LAN connections [1.2.1]
b. PC network configuration [1.2.2]
c. DSL router Quick Setup, via the Web-based management

3.2.1 Setting up WAN and LAN connections

WAN Connection
Your connection to the Internet by DSL(ADSL/VDSL) modem, connect its DSL socket to the wall socket using a telephone cable. If it has an Ethernet socket for the Wide Area Network (WAN), connect it to the external modem you have, or to the Ethernet socket you might have, using an Ethernet cable.
LAN Connection
Your computer can connect to the gateway in various forms (Ethernet, Wireless etc.), each requiring a different physical connection, if any in case of Wireless. The most common type of connection is Ethernet, with most platforms featuring four such ports. Use an Ethernet cable to connect between an Ethernet port on your DSL router and your computer's network card. Please refer to the accompanying Installation Guides for additional information.

3.2.2 PC Network Configuration

Each network interface on the PC should either be configured with a statically defined IP address and DNS address, or should be instructed to automatically obtain an IP address using the Network DHCP server. DSL router provides a DHCP server on its LAN and it is recommended to configure your LAN to obtain its IP and DNS server IP automatically.
This configuration principle is identical but performed differently on each operating system.
Figure 1.2 displays the 'TCP/IP Properties' dialog box as it appears in Windows XP. Following are TCP/IP configuration instructions for all supported operating systems.


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel
Figure 1.2: IP and DNS Configuration

. **Windows XP**
a. Access 'Network Connections' from the Control Panel.
b. Right click the Ethernet connection icon, and select 'Properties'.
c. Under the 'General' tab, select the 'Internet Protocol (TCP/IP)' component, and press the 'Properties' button.
d. The 'Internet Protocol (TCP/IP)' properties window will be displayed (see figure 1.2).
(a) Select the 'Obtain an IP address automatically' radio button.
(b) Select the 'Obtain DNS server address automatically' radio button.
(c) Click 'OK' to save the settings.
. **Windows 2000/98/Me**
a. Access 'Network and Dialing Connections' from the Control Panel.
b. Right click the Ethernet connection icon, and select 'Properties' to display the connection's properties.

c. Select the 'Internet Protocol (TCP/IP)' component, and press the 'Properties' button.
d. The 'Internet Protocol (TCP/IP)' properties will be displayed.
(a) Select the 'Obtain an IP address automatically' radio button.
(b) Select the 'Obtain DNS server address automatically' radio button.
(c) Click 'OK' to save the settings.

Windows NT

a. Access 'Network' from the Control Panel.
b. From the 'Protocol' tab, select the 'Internet Protocol (TCP/IP)' component, and press the 'Properties' button.
c. From the 'IP Address' tab select the 'Obtain an IP address automatically' radio button.
d. From the 'DNS' tab, verify that no DNS server is defined in the 'DNS Service Search Order' box and no suffix is defined in the 'Domain Suffix Search Order' box.

Linux

a. Login into the system as a super-user, by entering “su” at the prompt.
b. Type “ifconfig” to display the network devices and allocated IP addresses.
c. Type “pump -i <dev>”, where <dev> is the network device name.
d. Type “ifconfig” again to view the new allocated IP address.

e. Make sure no firewall is active on device <dev>.

4 Web-based Management

This chapter describes how to use DSL router Web-based management, which allows you to configure and control all of DSL router features and system parameters, using a user-friendly graphical interface. This user-friendly approach is also implemented in the WBM's documentation structure, which is based directly
on the WBM's structure. You will find it easy to correspondingly navigate through both the WBM and its documentation.

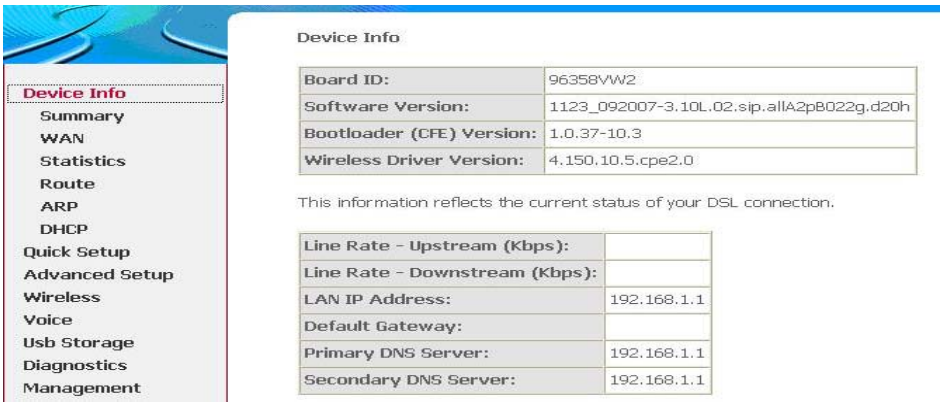


Figure 2.1: Web-based Management Home Page

4.1 Logging on the MODEM

The following introductions are prepared for the first time users, it is a detail “How-To” user guide.

4.1.1 First Time Logging

When logging into DSL router for the first time, the logging wizard is the first screen to appear.
a. Launch a Web browser on your computer.
b. Browse to “http://192.168.1.1” (DSL router default IP address).The logging page appears.
c. Enter a username and password. The default super username and password are both set to 'admin'(the common username and password are both “user”), you don’t need to input the username and password again if select the option “Remember my password”. It is recommended to change these default values after first time logging into the DSL router.
d. Click “OK” to login, or click “Cancel” to exit this login interface.

Figure 2.1.1: Web-based Management Login authentication page

After logging into the DSL router by a super username, you can query, configure, modify all configurations; and diagnose the system too.
You need to reboot the DSL router to enable your modification or configuration effective sometimes, e.g. you modified the PVC configuration; some modification can take effective at once without the MODEM being rebooted, such as adding a static route. See detailed descriptions below.

4.2 Quick Setup

When we enter into Quick Setup page, It mainly include three functions to do .

. WAN Interface setup

. LAN Interface setup

. Wireless Interface setup

'Quick Setup' enables speedy and accurate configuration of your Internet connection and other important parameters. The following sections describe these various configuration parameters. Whether you configure these parameters or use the default ones, click 'Next' to enable your Internet connection.

When subscribing to a broadband service, you should be aware of the method by which you are connected to the Internet. Your physical WAN device can be either Ethernet, DSL, or both. Technical information regarding the properties of your Internet connection should be provided by your Internet Service Provider (ISP). For example, your ISP should inform you whether you are connected to the Internet using a static or dynamic IP address, or what protocols, such as PPPOA or PPPoE, you will be using to communicate over the Internet.

4.2.1 WAN Interface Setup

In WAN Interface Setup phase, We mainly setup a PVC and the property of this PVC:

. VPI

. VCI

. Qos

. Internet Connection Type

. Encapsulation Type

. IGMP service

. NAT

4.2.1.1 Setup VPI/VCI and QoS

After logging into the DSL router, When we were not config any PVC at privious time and we have not default settings include PVC,you will see a “Quick Setup” web page, which will include some basic configuration that is needed by ATM PVC. the following introductions will guide you through the steps

necessary to configure your DSL Router.
According to your Internet service providers (ISP) instructions, specify the following parameters:

.VPI (Virtual Path Identifier):

The virtual path between two points in an ATM network, and its valid value is from 0 to 255.

.VCI (Virtual Channel Identifier):

The virtual channel between two points in an ATM network, ranging from 32 to 65535 (1 to 31 are reserved for known protocols).

.Enable Quality Of Service:

Enabling QoS for a PVC improves performance for selected classes of applications. However, since QoS also consumes system resources, the number of PVCs will be reduced consequently. Use Advanced Setup/Quality of Service to assign priorities for the applications.

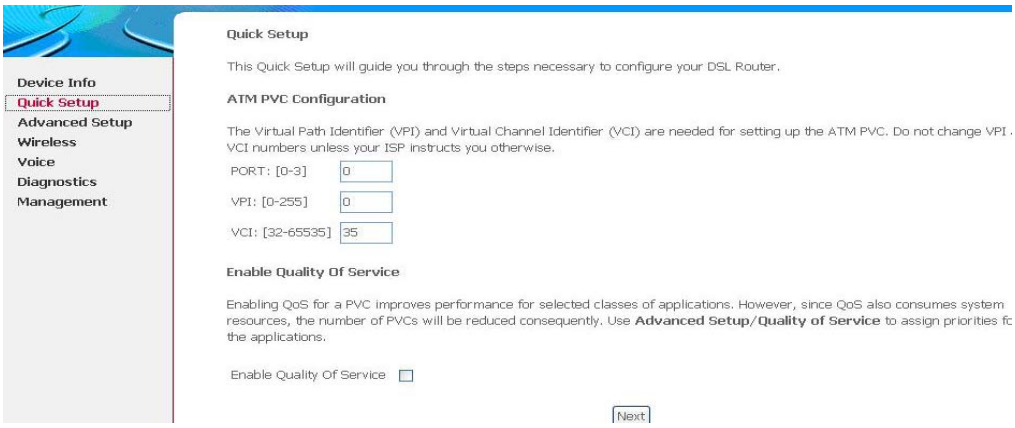

Device Info
Quick Setup
Advanced Setup
Wireless
Voice
Diagnostics
Management
Quick Setup
This Quick Setup will guide you through the steps necessary to configure your DSL Router.
ATM PVC Configuration
The Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) are needed for setting up the ATM PVC. Do not change VPI and VCI numbers unless your ISP instructs you otherwise.
PORT: [0-3] 0
VPI: [0-255] 0
VCI: [32-65535] 35
Enable Quality Of Service
Enabling QoS for a PVC improves performance for selected classes of applications. However, since QoS also consumes system resources, the number of PVCs will be reduced consequently. Use Advanced Setup/Quality of Service to assign priorities fc the applications.
Enable Quality Of Service
Next

Figure 2.2.1: PVC and it's Qos config page

For example, PVC 0/35 is required to modify, so QoS will remain default values. In actual applications, you can modify them depending on your ISP told you.

4.2.1.2 Select Internet Connection Type and Encapsulation Type

You can selecting your connection type from the following list, each connect type has it's Encapsulation Type:

.PPP over ATM (PPPoA)
    PPPoA Encapsulation Mode:
    .VC/MUX
    .LLC/ENCAPSULATION
.PPP over Ethernet (PPPoE)
    PPPoE Encapsulation Mode:
    .LLC/SNAP-BRIDGING
    .VC/MUX
.MAC Encapsulation Routing (MER)
    MER Encapsulation Mode:
    .LLC/SNAP-BRIDGING
    .VC/MUX
.IP over ATM (IPoA)
    IPoA Encapsulation Mode:
    .LLC/SNAP-ROUTING
    .VC/MUX
.Bridging
    Bridging Encapsulation Mode:
    .LLC/SNAP-BRIDGING
    .VC/MUX

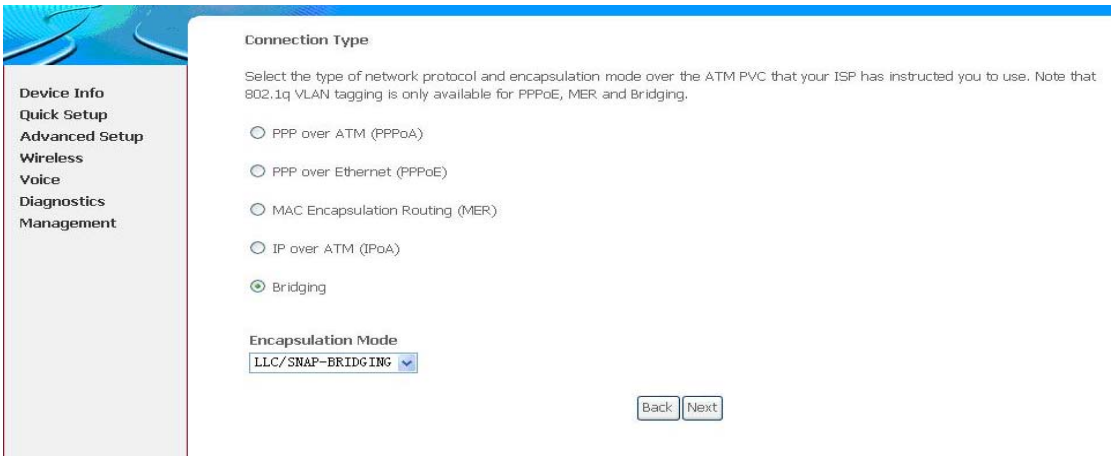


Figure 2.2.2: Internet Connection Type and Encapsulation Type page

For example, Change the connection type of PVC 0/35 to “bridge”. Select “bridging”, and “LLC/SNAP-BRIDGING” (depending on the uplink equipment, generally “LLC/SNAP-BRIDGING”) as “Encapsulation Mode”.

4.2.1.3 Internet Connection Type-PPP over ATM (PPPoA)

A. From Figure 2.2.1 config PVC and Qos of Pvc;
B. From Figure 2.2.2 Select '.PPP over ATM (PPPoA)' from the 'Connection Type' box and It’s Encapsulation Type from the ' Encapsulation Mode' combo box:

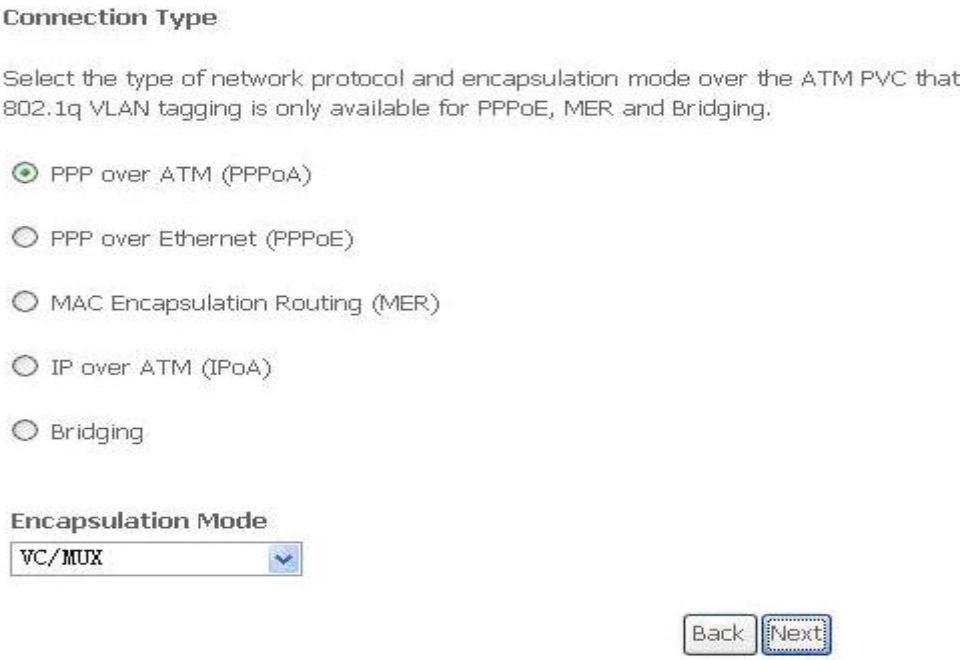

Connection Type
Select the type of network protocol and encapsulation mode over the ATM PVC that 802.1q VLAN tagging is only available for PPPoE, MER and Bridging.
PPP over ATM (PPPoA)
PPP over Ethernet (PPPoE)
MAC Encapsulation Routing (MER)
IP over ATM (IPoA)
Bridging
Encapsulation Mode
VC/MUX
Back
Next

Figure 2.2.2.1.1 PPP over ATM (PPPoA)

C. We click ‘Next’ button enter PPP information config page:

PPP Username and Password
PPP usually requires that you have a user name and password to establish your name and password that your ISP has provided to you.
PPP Username:
PPP Password:
Authentication Method:
AUTO
Dial on demand (with idle timeout timer)
Inactivity Timeout (minutes) [1-4320]:
0
PPP IP extension
Advanced DMZ
Non DMZ IP Address:
Non DMZ Net Mask:
Use Static IP Address
IP Address:
Retry PPP password on authentication error
Enable PPP Debug Mode
Back
Next

Figure 2.2. 2.1.2 PPP information and others funtion page

Your Internet Service Provider (ISP) should provide you with the following information:
. PPP Username
. PPP Password
. Authentication Method
You can also select another service function as below:
. Dial on demand (with idle timeout timer)
. PPP IP extension
. Use Static IP Address
. Retry PPP password on authentication error
. Enable PPP Debug Mode

D. We click 'Next' button enter wan and Igmp function information config page:
If you want to use IGMP service on pppoa pvc,we must select 'Enable IGMP Multicast' box.

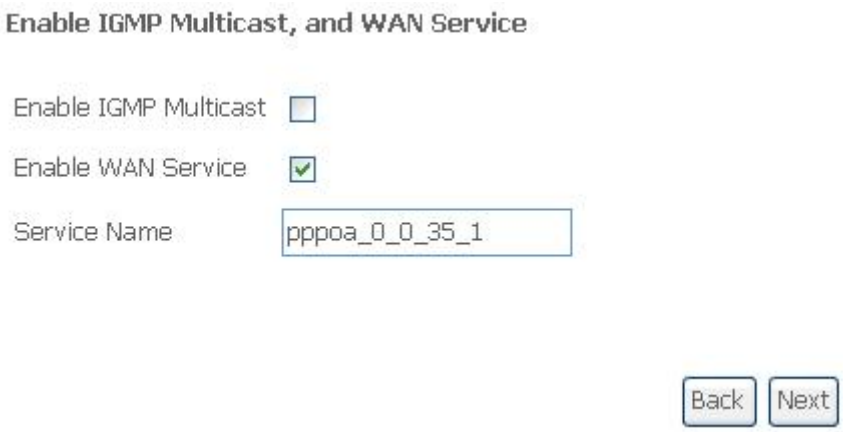


Figure 2.2. 2.1.3 PPPoA IGMP and WAN service page

4.2.1.4 Internet Connection Type-PPP over Ethernet (PPPoE)

A. From Figure 2.2.1 config PVC and Qos of Pvc;

B. From Figure 2.2.2 Select '.PPP over Ethernet (PPPoE)' from the 'Connection Type' box and It's Encapsulation Type from the ' Encapsulation Mode' combo box:

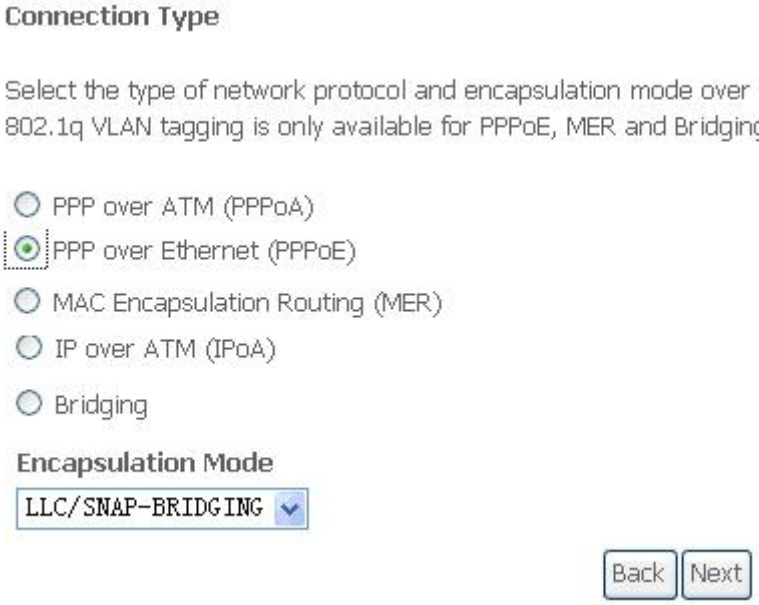


Figure 2.2.2.2.1 PPP over Ethernet (PPPoE)

C. We click 'Next' button enter PPP information config page:

PPP Username and Password
PPP usually requires that you have a user name and password to establish your name and password that your ISP has provided to you.
PPP Username:
PPP Password:
Authentication Method:
AUTO
Dial on demand (with idle timeout timer)
Inactivity Timeout (minutes) [1-4320]:
0
PPP IP extension
Advanced DMZ
Non DMZ IP Address:
Non DMZ Net Mask:
Use Static IP Address
IP Address:
Retry PPP password on authentication error
Enable PPP Debug Mode
Back
Next

Figure 2.2. 2.2.2 PPP information and others funtion page

Your Internet Service Provider (ISP) should provide you with the following information:
. PPP Username
. PPP Password
. Authentication Method
You can also select another service function as below:
. Dial on demand (with idle timeout timer)
. PPP IP extension
. Use Static IP Address
. Retry PPP password on authentication error
. Enable PPP Debug Mode

D. We click 'Next' button enter wan and Igmp function information config page:
If you want to use IGMP service on pppoa pvc,we must select 'Enable IGMP Multicast' box.

Figure 2.2. 2.2.3 PPPoE IGMP and WAN service page

4.2.1.5 Internet Connection Type-MAC Encapsulation Routing (MER)

A. From Figure 2.2.1 config PVC and Qos of Pvc;

B. From Figure 2.2.2 Select 'MAC Encapsulation Routing (MER)' from the 'Connection Type' box and It's Encapsulation Type from the ' Encapsulation Mode' combo box:

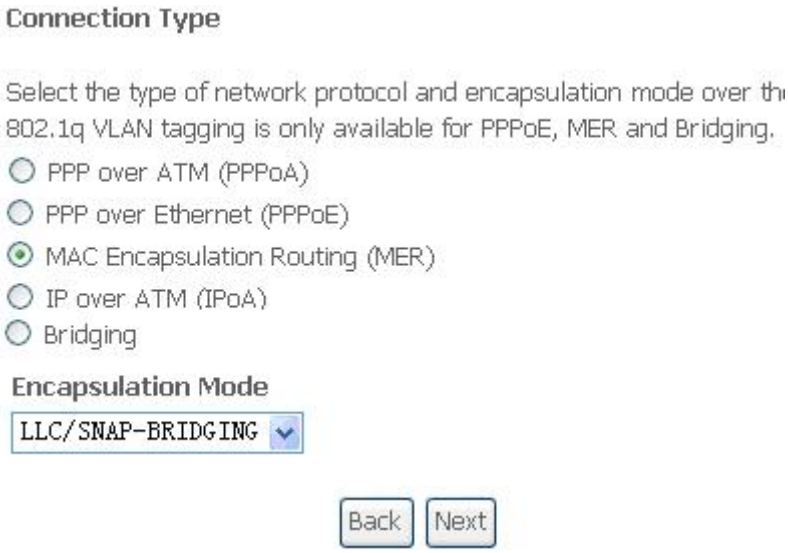


Figure 2.2.2.3.1 MAC Encapsulation Routing (MER)

C. We click 'Next' button enter WAN IP information config page:

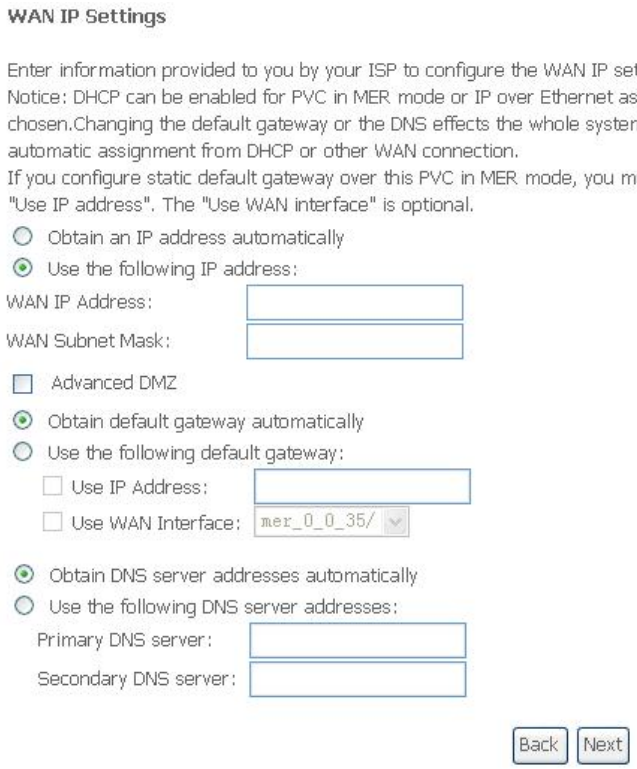

WAN IP Settings
Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: DHCP can be enabled for PVC in MER mode or IP over Ethernet as WAN interface if "Obtain an IP address automatically" chosen.Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection.
If you configure static default gateway over this PVC in MER mode, you must enter the IP address of the remote gateway in the "Use IP address". The "Use WAN interface" is optional.
Obtain an IP address automatically
Use the following IP address:
WAN IP Address:
WAN Subnet Mask:
Advanced DMZ
Obtain default gateway automatically
Use the following default gateway:
Use IP Address:
Use WAN Interface:
mer_0_0_35/
Obtain DNS server addresses automatically
Use the following DNS server addresses:
Primary DNS server:
Secondary DNS server:
Back
Next

Figure 2.2.2.3.2 WAN IP config page

Your Internet Service Provider (ISP) should provide you with the following
You can also select another service function as below:
. Obtain an IP address automatically (use dhcp to obtain wan ip)
. Use the following IP address (use static wan ip)
. Advanced DMZ
. Obtain default gateway automatically (use dhcp to obtain gateway ip)
. Use the following default gateway (use static gateway ip)
. Obtain DNS server addresses automatically (use dhcp to obtain DNS server ip)
. Use the following DNS server addresses (use static DNS server ip)

D. We click 'Next' button enter wan and Igmp function information config page:
If you want to use IGMP service on MER pvc,we must select 'Enable IGMP Multicast' box.
In MER mode, There are some functions:
. Enable NAT
. Enable Fullcone NAT
. Enable Firewall

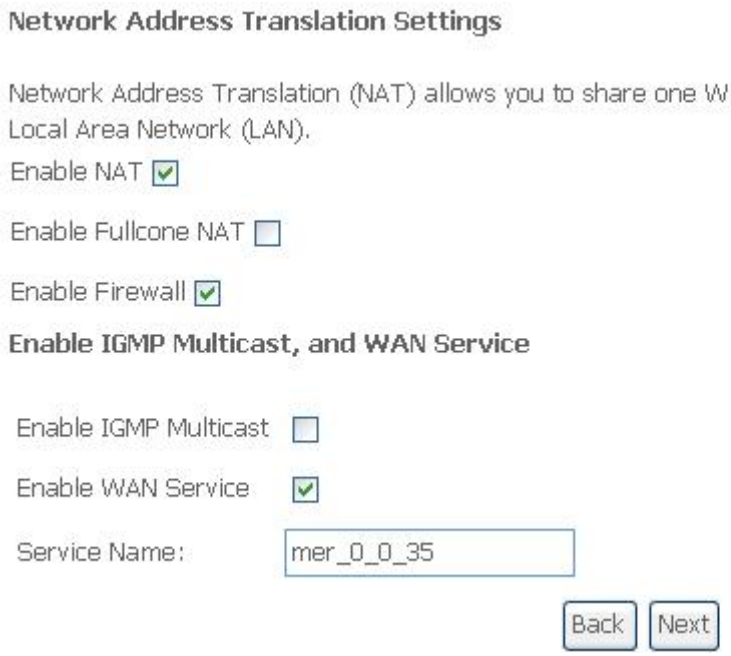


Figure 2.2.2.3.3 MER IGMP and WAN service page

4.2.1.6 Internet Connection Type-IP over ATM (IPoA)

A. From Figure 2.2.1 config PVC and Qos of Pvc;

B. From Figure 2.2.2 Select ' IP over ATM (IPoA)' from the 'Connection Type' box and It's Encapsulation Type from the ' Encapsulation Mode' combo box:

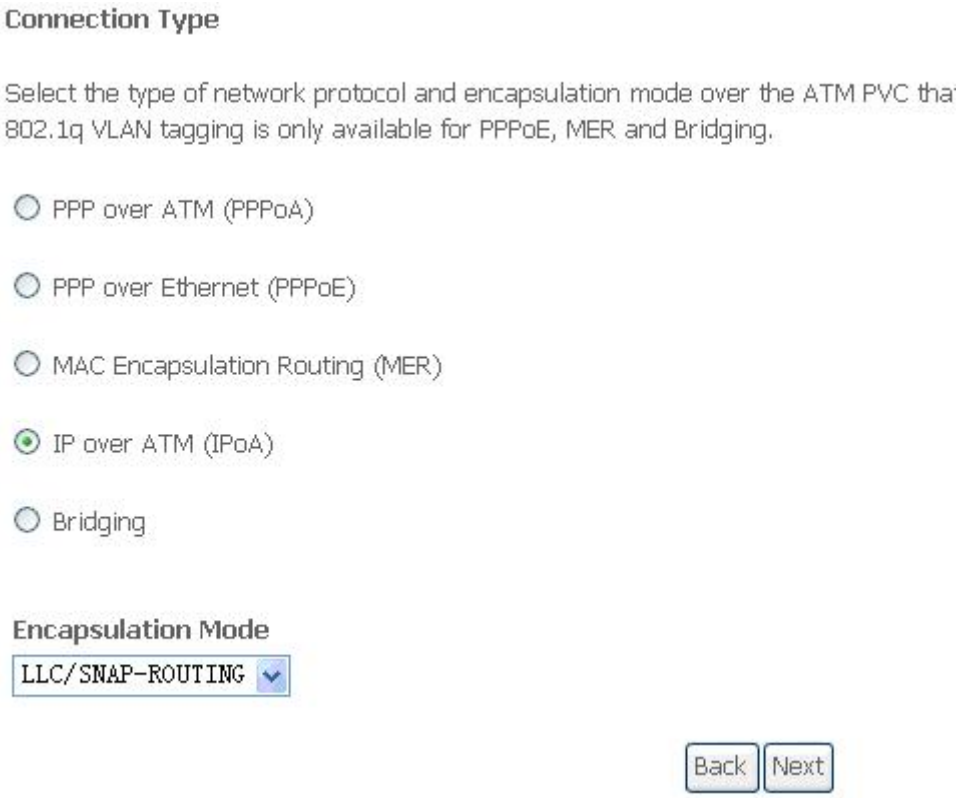

Connection Type
Select the type of network protocol and encapsulation mode over the ATM PVC tha
802.1q VLAN tagging is only available for PPPoE, MER and Bridging.
PPP over ATM (PPPoA)
PPP over Ethernet (PPPoE)
MAC Encapsulation Routing (MER)
IP over ATM (IPoA)
Bridging
Encapsulation Mode
LLC/SNAP-ROUTING
Back
Next

Figure 2.2.2.4.1 IP over ATM (IPoA)

C. We click 'Next' button enter WAN IP information config page:

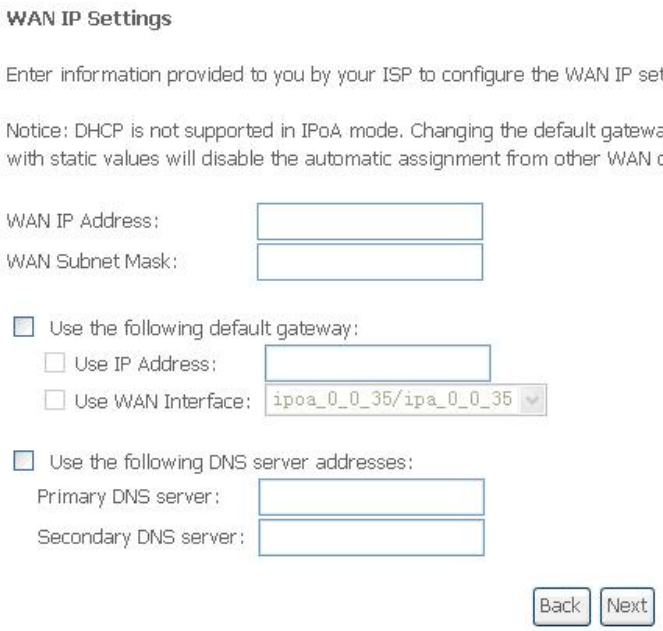

WAN IP Settings
Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: DHCP is not supported in IPoA mode. Changing the default gateway or the DNS effects the whole system.
with static values will disable the automatic assignment from other WAN connection.
WAN IP Address:
WAN Subnet Mask:
Use the following default gateway:
Use IP Address:
Use WAN Interface:
ipoa_0_0_35/ipa_0_0_35
Use the following DNS server addresses:
Primary DNS server:
Secondary DNS server:
Back
Next

Figure 2.2.2.4.2 WAN IP config page

Your Internet Service Provider (ISP) should provide you with the following
You can also select another service function as below:
. Use the following IP address (static wan ip)
. Use the following default gateway (static gateway ip)
. Use the following DNS server addresses (static DNS server ip)

D. We click 'Next' button enter wan and Igmp function information config page:
If you want to use IGMP service on ipoa pvc,we must select 'Enable IGMP Multicast' box.
In MER mode, There are some functions:
. Enable NAT
. Enable Fullcone NAT
. Enable Firewall

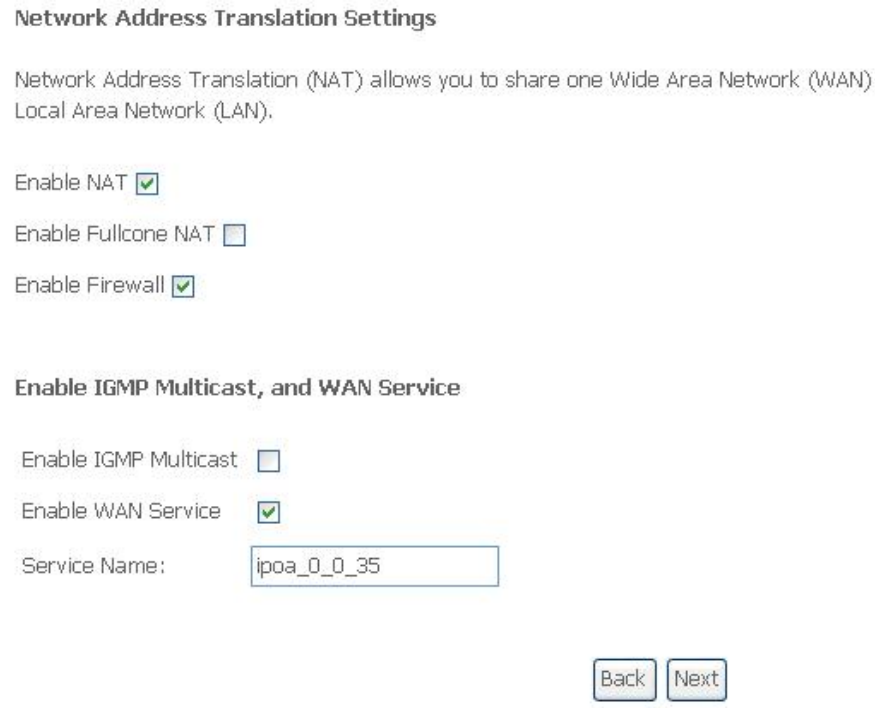


Figure 2.2.2.4.3 IPOA IGMP and WAN service page

4.2.1.7 Internet Connection Type-Bridging

A. From Figure 2.2.1 config PVC and Qos of Pvc;
B. From Figure 2.2.2 Select ' IP over ATM (IPoA)' from the 'Connection Type' box and It's Encapsulation Type from the ' Encapsulation Mode' combo box:

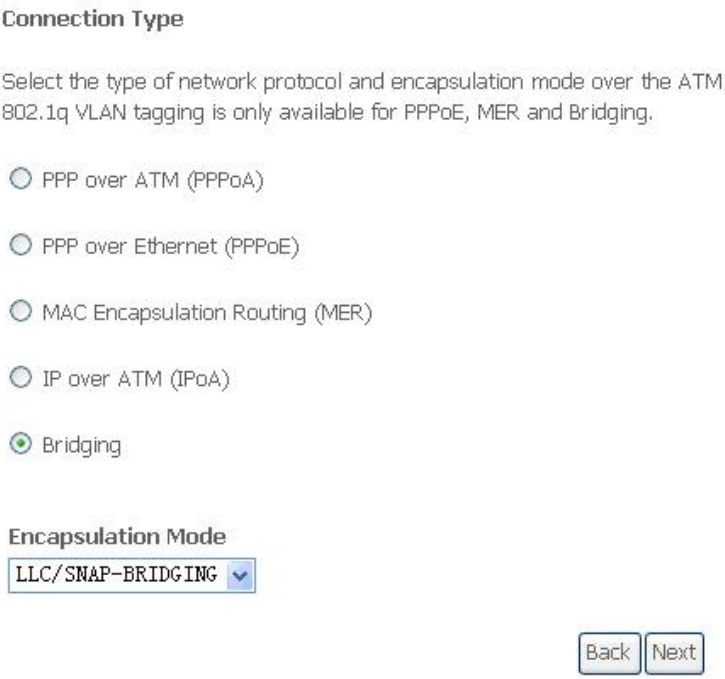

Connection Type
Select the type of network protocol and encapsulation mode over the ATM PVC that your ISP has instructed y
802.1q VLAN tagging is only available for PPPoE, MER and Bridging.
PPP over ATM (PPPoA)
PPP over Ethernet (PPPoE)
MAC Encapsulation Routing (MER)
IP over ATM (IPoA)
Bridging
Encapsulation Mode
LLC/SNAP-BRIDGING
Back
Next

Figure 2.2.2.5.1 Bridging

C. We click 'Next' button enter wan a function information config page:

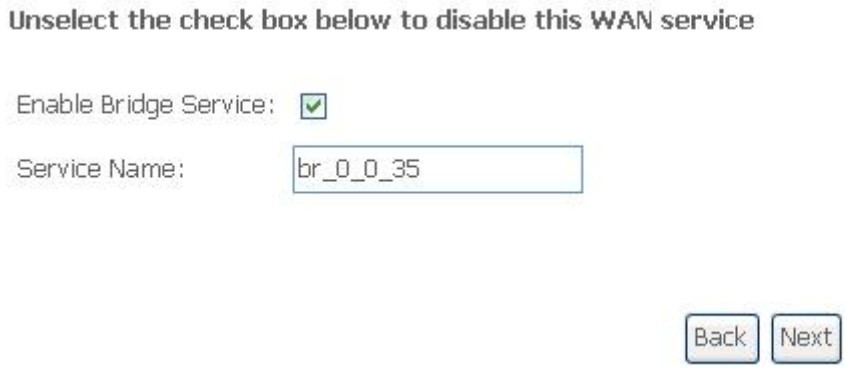


Figure 2.2.2.5.2 Bridging service page

4.2.2 LAN Inerface Setup

In Lan interface setup page,

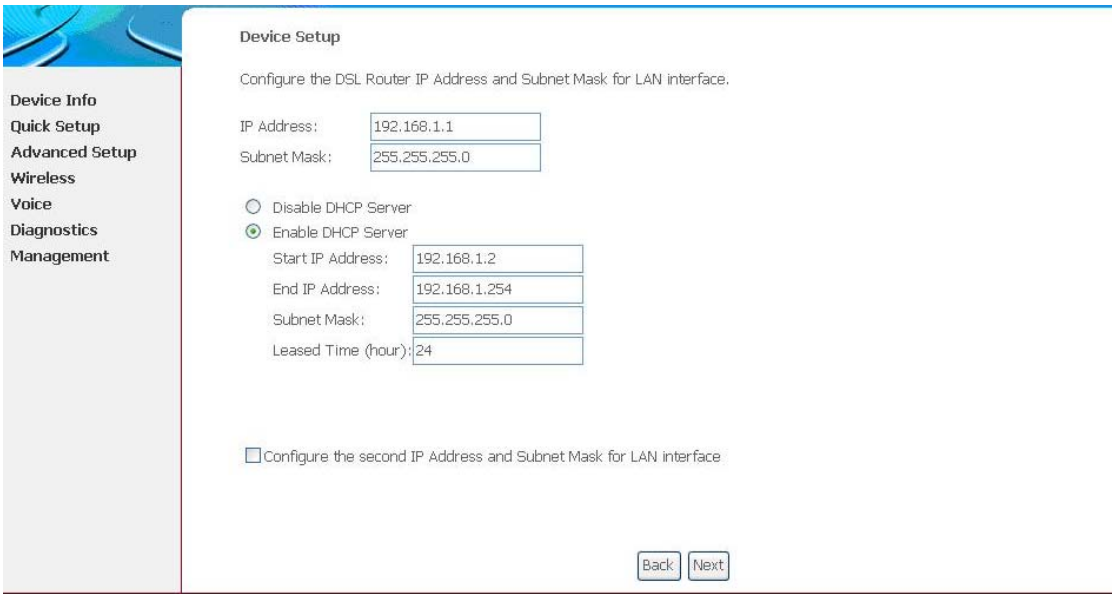


Figure 2.2.2.5.3:LAN Interface Setup

4.2.3 Wireless Interface Setup

Enable Wireless: Check or uncheck this box to enable or disable the wireless connection.
SSID: The SSID is the network name shared among all points in a wireless network. The SSID must be identical for all points in the wireless network. It is case-sensitive and must not exceed 32 characters (use any of the characters on the keyboard). Make sure this setting is the same for all points in your wireless network.

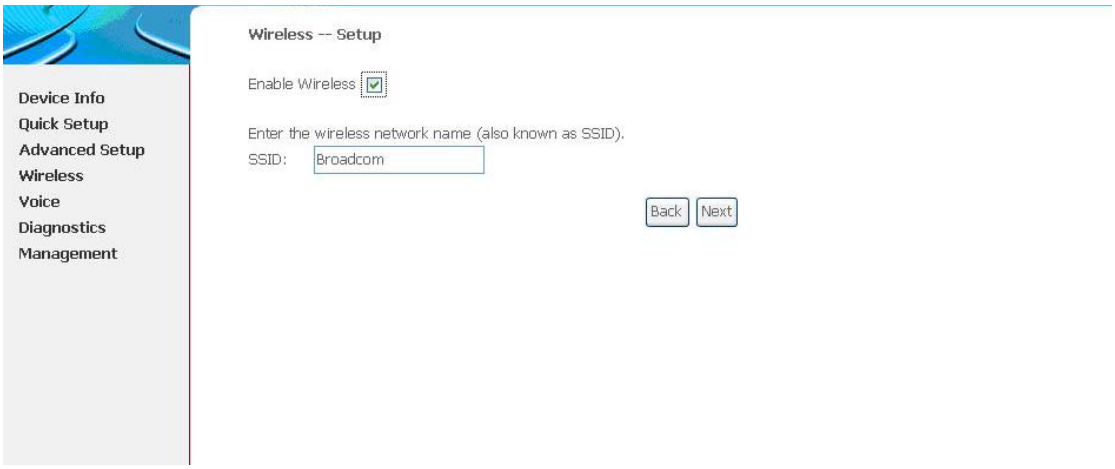


Figure 2.2.2.5.4:Wireless Setup

4.2.4 WAN Setup Summary

When In WAN setup summary phase, The property of the PVC added can view:
. VPI/VCI
. Connection Type:
. Service Name:
. Service Category:
. IP Address:
. Service State:

. NAT
. Firewall
. IGMP
. QOS

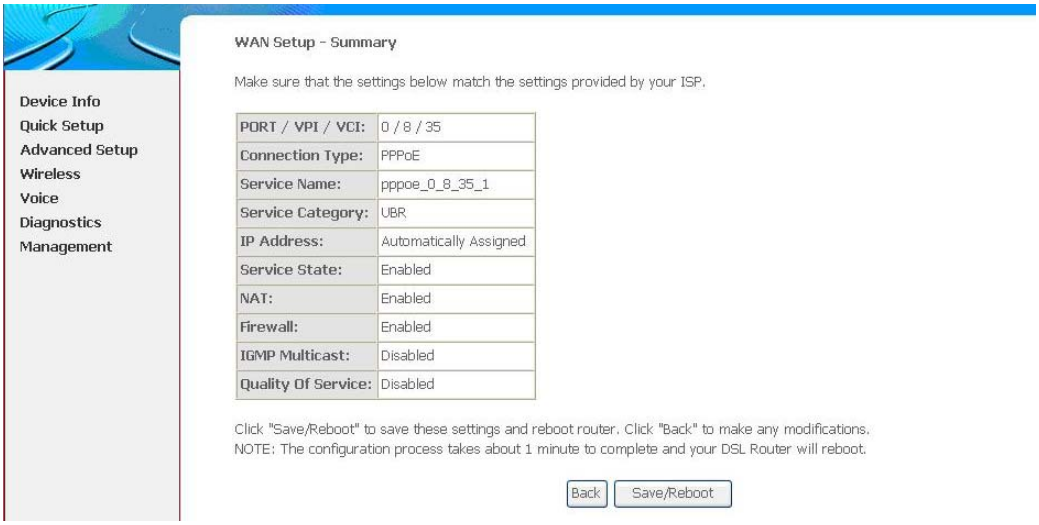

Device Info
Quick Setup
Advanced Setup
Wireless
Voice
Diagnostics
Management
WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
PORT / VPI / VCI: 0 / 8 / 35
Connection Type: PPPoE
Service Name: pppoe_0_8_35_1
Service Category: UBR
IP Address: Automatically Assigned
Service State: Enabled
NAT: Enabled
Firewall: Enabled
IGMP Multicast: Disabled
Quality Of Service: Disabled
Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.
Back
Save/Reboot

Figure 2.2.2.5.5: WAN setup summary

Click “Save” to save these settings.And you can click “Back” to make any modifications. After you click “Save/Reboot”, it show the following interface.

NOTE: You need to reboot to activate this WAN interface and further configure services over this interface， and it will take about two minutes to done with it .

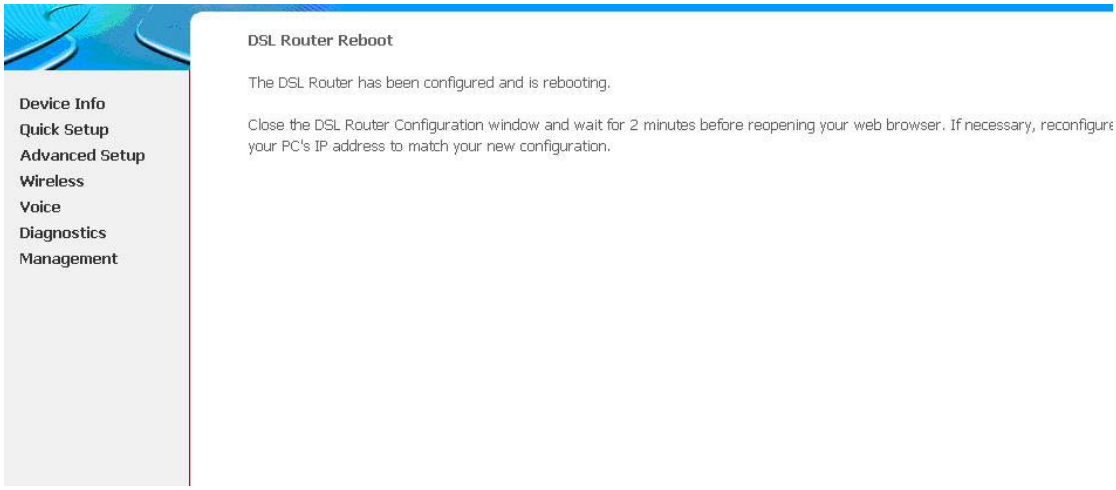

Device Info
Quick Setup
Advanced Setup
Wireless
Voice
Diagnostics
Management
DSL Router Reboot
The DSL Router has been configured and is rebooting.
Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure
your PC's IP address to match your new configuration.

Figure 2.2.2.5.6:DSL Router Reboot

4.2.5 Quick Setup Completed

DSL router does not require further configuration in order to start working. After the setup described in this chapter, you can immediately start using your gateway to:

. Share a broadband connection among multiple users (HTTP, FTP, Telnet, NetMeeting) and between all of the computers connected to your home network.
. Build a home network by connecting additional PCs and network devices to the gateway.
. Control network parameters, including DHCP, DNS and WAN settings.
. View network status, traffic statistics, system log and more.
. Allow access from the Internet to games and other services provided by computers in the home network.
. Prohibit computers in the home network from accessing selected services on the Internet.

. Block access to specific Internet Web sites from your home network.To learn about how to configure your Firewall security parameters, please refer to section 7.3. If you wish to apply corporate-grade security to your network, please refer to section 7.3.11.
If your gateway is equipped with multiple LAN ports, you can connect additional devices directly to the gateway. Otherwise, connect a hub or switch to the LAN port, to which you can connect additional devices.In both cases, configure newly connected devices to automatically obtain IP address as described above.

4.3 DSL Router Device information

Click “Device Info”, It should view the information as below:

. Summary

. WAN

. Statistics

. Route

. ARP

. DHCP

Figure 2.3 Device Information Menu

4.3.1 Summary of Device information

This interface contains the following information:

. Board ID:

. Software Version:

. Bootloader (CFE) Version:

. Wireless Driver Version:

. Upstream Line Rate

. Downstream Line Rate

. LAN IP Address: The management IP address

. Default Gateway :No gateway in a pure bridging mode; under other modes such as PPPOE/PPPOA, it is the address of the uplink equipment.

. DNS Server address: Obtained from the uplink equipment in PPPOE/PPPOA mode; No DNS Server address in a pure bridging mode; or input them manually.

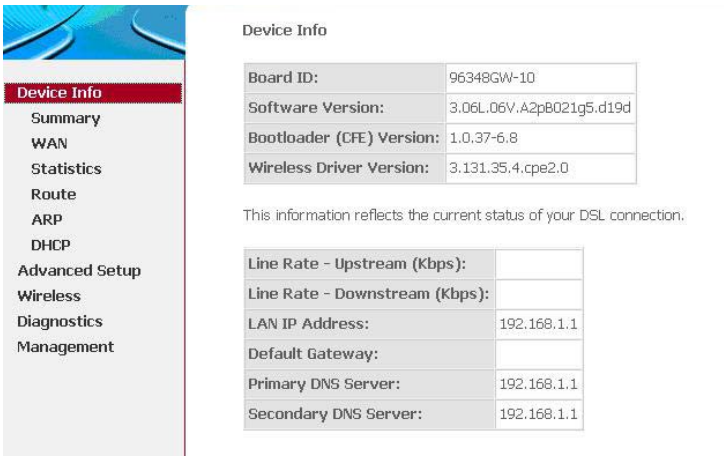


Figure 2.3.1 summary of Device information

4.3.2 WAN Interface information

Click “WAN” to show the following interface, depend on the selected connection mode, the Summary screen shows the status and also the connect or disconnect button.
This interface contains the following informations of every wan connection:

. VPI/VCI
. VLAN
. Connection ID
. Category
. Service
. Interface
. Protocol
. IGMP
. Qos
. State
. Status
. IP address

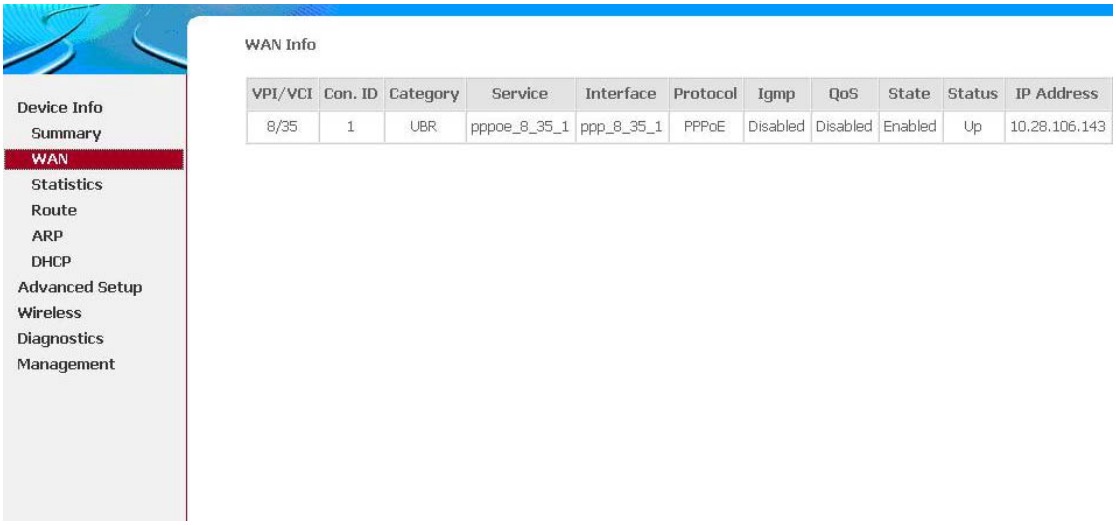


Figure 2.3.2 WAN interface info

4.3.3 Statistics

In this page, It include four parts information:

. Statistics of LAN

. Statistics of WAN

. Statistics of ATM

. Statistics of ADSL

4.3.4 Statistics of LAN

Click “Statistics”-->”LAN” to show the following interface. You can query information on packets recevied at the Ethernet, USB and Wireless interfaces. Click “Reset Statistics” to return the values to zero and recount them.

Lan side interface included Ethernet USB and wireless device,each device you can view info as below:

. Interface

. Received

Bytes: Bytes of Received

Pkts: Packets of Received

Errs: Errors packets of Received

Drops: Drops packets of Received

. Transmitted

Bytes: Bytes of Received

Pkts: Packets of Received

Errs: Errors packets of Received

Drops: Drops packets of Received

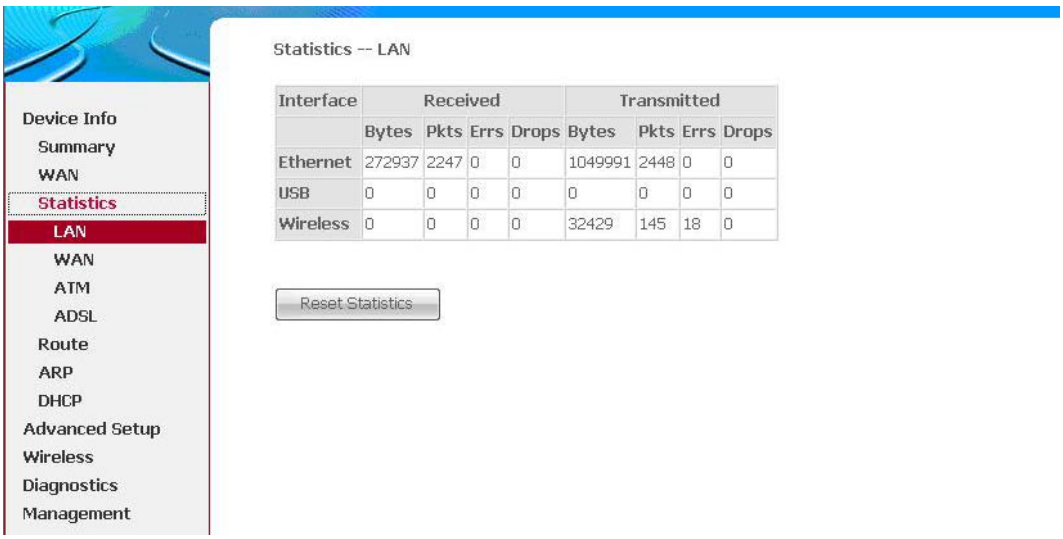


Figure 2.3.4 Statistics of LAN

4.3.5 Statistics of WAN

Click “Statistics”-->”WAN” to show the following interface. You can query information on packets recevied at the WAN interfaces. Click “Reset Statistics” to return the values to zero and recount them.

Informations as below:

. Service

. VPI/VCI

. Protocol

. Interface

. Received

Bytes: Bytes of Received

Pkts: Packets of Received

Errs: Errors packets of Received
Drops: Drops packets of Received

. Transmitted
Bytes: Bytes of Received
Pkts: Packets of Received
Errs: Errors packets of Received
Drops: Drops packets of Received

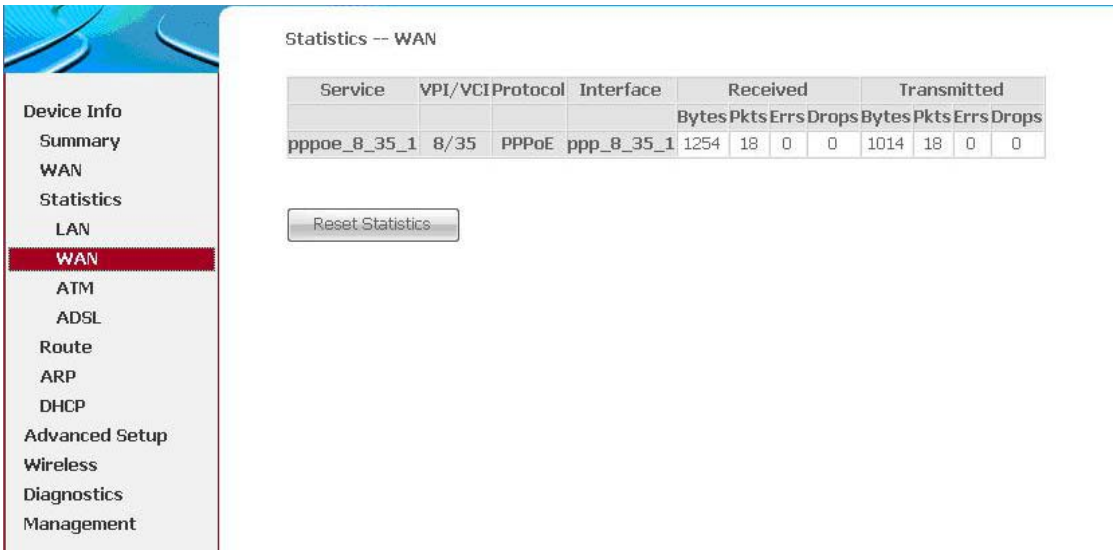


Figure 2.3.5 Statistics of WAN

4.3.6 Statistics of ATM

Click “Statistics”-->”ATM” to show the following interface. You can query information on packets recevied at the ATM interfaces. Click “Reset” to return the values to zero and recount them.
There are three part info:

. ATM Interface Statistics:
In Octets
Out Octets
In Errors
In Unknown
In Hec Errors
In Invalid Vpi Vci Errors
In Port Not Enable Errors
In PTI Errors
In Idle Cells In Circuit Type Errors
In OAM RM CRC Errors
In GFC Errors

. AAL5 Interface Statistics:
In Octets
Out Octets
In Ucast Pkts
Out Ucast Pkts
In Errors
Out Errors
In Discards
Out Discards

. AAL5 VCC Statistics:
VPI/VCI
CRC Errors
SAR Timeouts

Oversized SDUs
Short Packet Errors
Length Errors

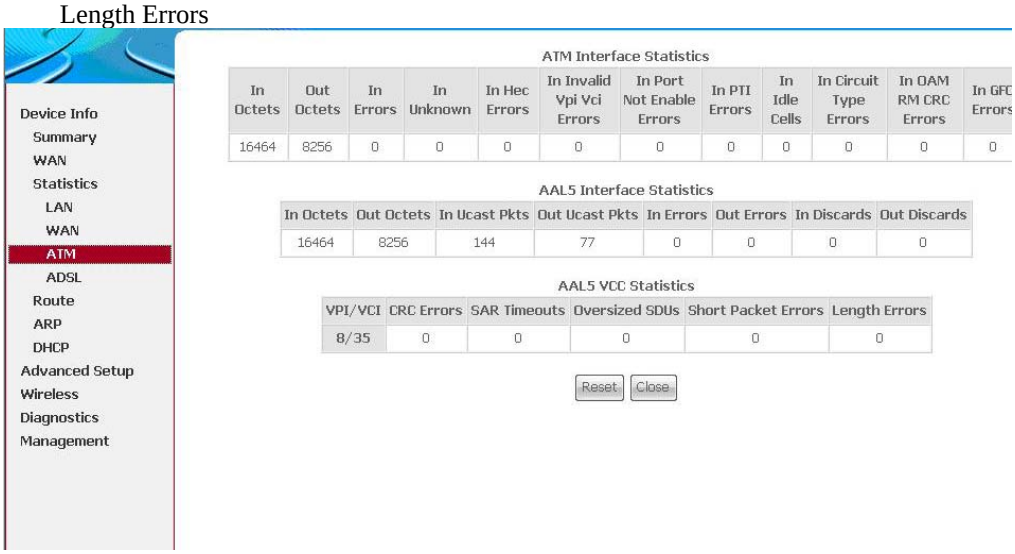

Device Info
Summary
WAN
Statistics
LAN
WAN
ATM
ADSL
Route
ARP
DHCP
Advanced Setup
Wireless
Diagnostics
Management
ATM Interface Statistics
In Octets | Out Octets | In Errors | In Unknown | In Hec Errors | In Invalid Vpi Vci Errors | In Port Not Enable Errors | In PTI Errors | In Idle Cells | In Circuit Type Errors | In OAM RM CRC Errors | In GFC Errors
16464 | 8256 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0
AAL5 Interface Statistics
In Octets | Out Octets | In Ucast Pkts | Out Ucast Pkts | In Errors | Out Errors | In Discards | Out Discards
16464 | 8256 | 144 | 77 | 0 | 0 | 0 | 0
AAL5 VCC Statistics
VPI/VCI | CRC Errors | SAR Timeouts | Oversized SDUs | Short Packet Errors | Length Errors
8/35 | 0 | 0 | 0 | 0 | 0
Reset
Close

Figure 2.3.6 Statistics of ATM

4.3.7 Statistics of ADSL

Click “Statistics”-->”ADSL” to show the following interface.
If the DSL line is activated, the following window will show.

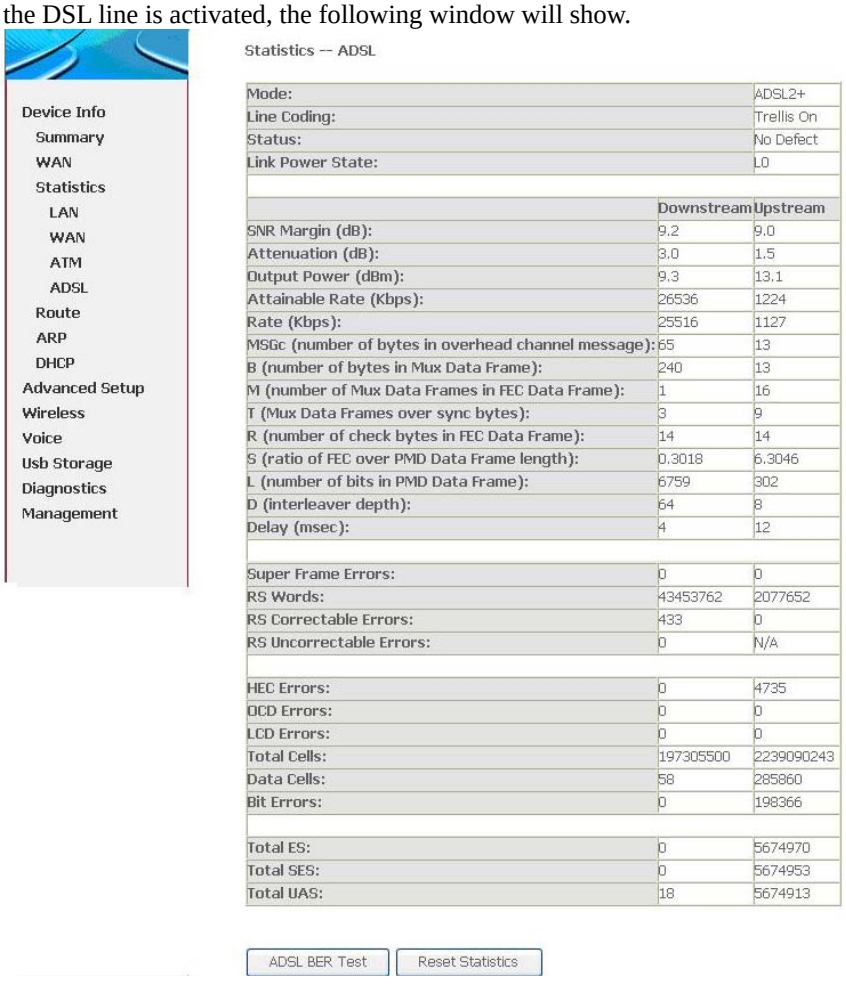

Device Info
Summary
WAN
Statistics
LAN
WAN
ATM
ADSL
Route
ARP
DHCP
Advanced Setup
Wireless
Voice
Usb Storage
Diagnostics
Management
Statistics -- ADSL
Mode: ADSL2+
Line Coding: Trellis On
Status: No Defect
Link Power State: L0
Downstream | Upstream
SNR Margin (dB): 9.2 | 9.0
Attenuation (dB): 3.0 | 1.5
Output Power (dBm): 9.3 | 13.1
Attainable Rate (Kbps): 26536 | 1224
Rate (Kbps): 25516 | 1127
MSGc (number of bytes in overhead channel message): 65 | 13
B (number of bytes in Mux Data Frame): 240 | 13
M (number of Mux Data Frames in FEC Data Frame): 1 | 16
T (Mux Data Frames over sync bytes): 3 | 9
R (number of check bytes in FEC Data Frame): 14 | 14
S (ratio of FEC over PMD Data Frame length): 0.3018 | 6.3046
L (number of bits in PMD Data Frame): 6759 | 302
D (interleaver depth): 64 | 8
Delay (msec): 4 | 12
Super Frame Errors: 0 | 0
RS Words: 43453762 | 2077652
RS Correctable Errors: 433 | 0
RS Uncorrectable Errors: 0 | N/A
HEC Errors: 0 | 4735
OCD Errors: 0 | 0
LCD Errors: 0 | 0
Total Cells: 197305500 | 2239090243
Data Cells: 58 | 285860
Bit Errors: 0 | 198366
Total ES: 0 | 5674970
Total SES: 0 | 5674953
Total UAS: 18 | 5674913
ADSL BER Test
Reset Statistics

Figure 2.3.7 Statistics of ADSL

You will see the following information pertinent to the ADSL line in the page:
. Mode: G.DMT/G.LITE/T1.413/ADSL 2+/ADSL 2/READSL2
. Line Coding: Trallis on, etc.
. Status: Link Down, No Defect, Training
. Link Power State: L0, L1, L2
. Rate (Kbps): Upstream Line Rate/Downstream Line Rate.
At the lower part of this interface, there is a “Reset Statistics” button. Click it to return values to zero and recount.

4.3.7.1 ADSL BER Test

Click “ADSL BER Test” to do a “Bit Error Rate” Test on the DSL line. The test interface is as follows:

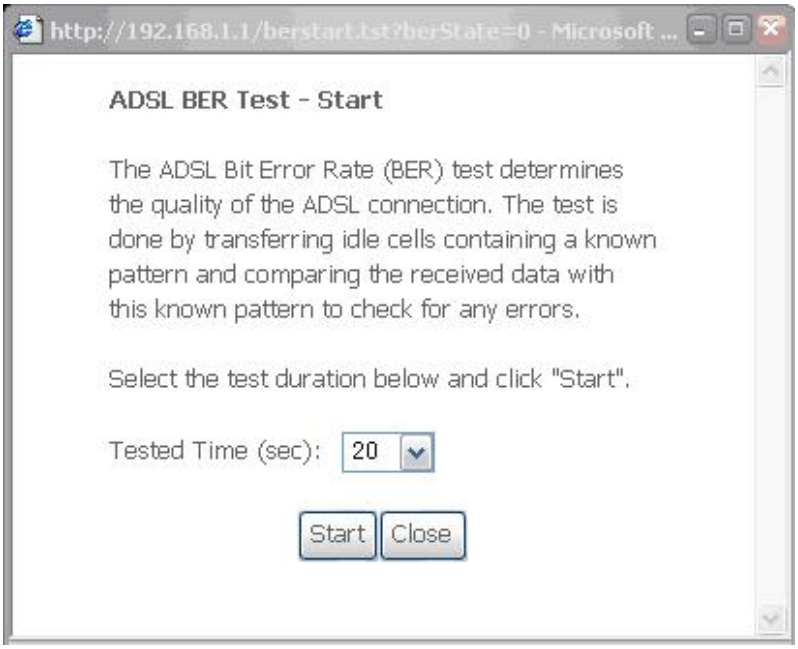

http://192.168.1.1/berstart.tst?berState=0 - Microsoft ...
ADSL BER Test - Start
The ADSL Bit Error Rate (BER) test determines the quality of the ADSL connection. The test is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for any errors.
Select the test duration below and click "Start".
Tested Time (sec): 20
Start
Close

Figure 2.3.7.1 ADSL BER Test

The Tested Time (sec) has the following choices: 1, 5, 10, 20, 60, 120, 180, 240, 300, and 360. Select a time and then click “Start” to pop up the following interfaces in sequence.

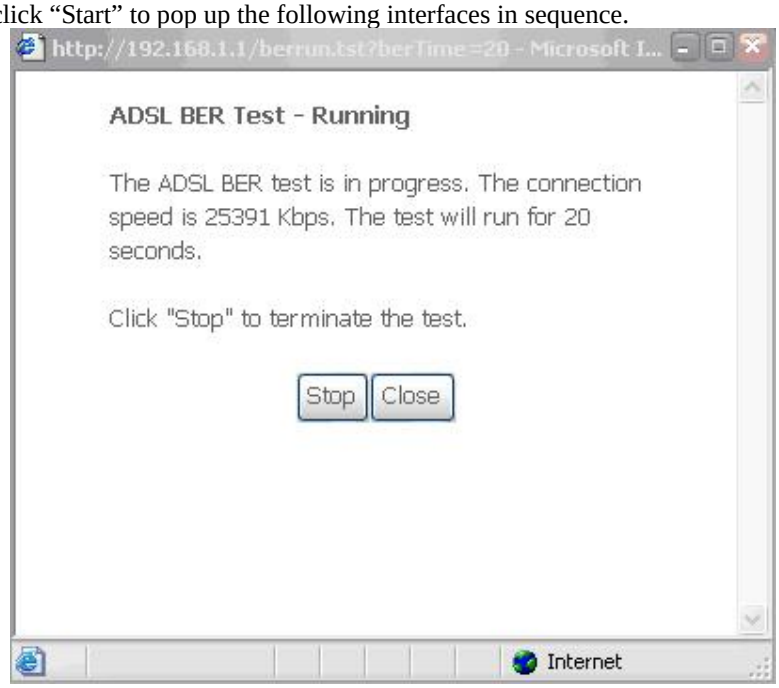

http://192.168.1.1/berrun.tst?berTime=20 - Microsoft I...
ADSL BER Test - Running
The ADSL BER test is in progress. The connection speed is 25391 Kbps. The test will run for 20 seconds.
Click "Stop" to terminate the test.
Stop
Close
Internet

Figure 2.3.7.1 ADSL BER Test Running Page

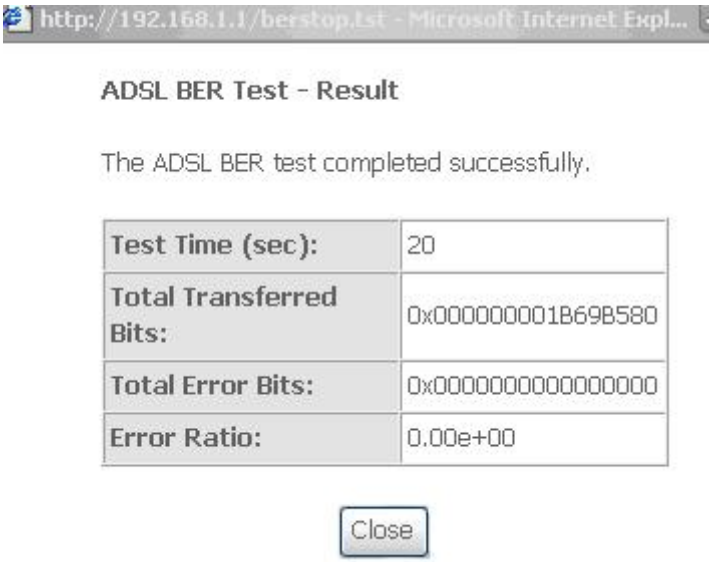

http://192.168.1.1/berstop.tst - Microsoft Internet Expl...
ADSL BER Test - Result
The ADSL BER test completed successfully.
Test Time (sec): 20
Total Transferred Bits: 0x000000001B69B580
Total Error Bits: 0x0000000000000000
Error Ratio: 0.00e+00
Close

Figure 2.3.7.1 ADSL BER Test Result

Note: If the error ratio reaches up to “e-5”, the user will not be able to access the Internet.

4.3.8 Route table information

Click “Route”. You can view the route table information,Each route item in route table has info as below:
. Destination
. Gateway
. Subnet Mask
. Flag
. Metric
. Service
. Interface

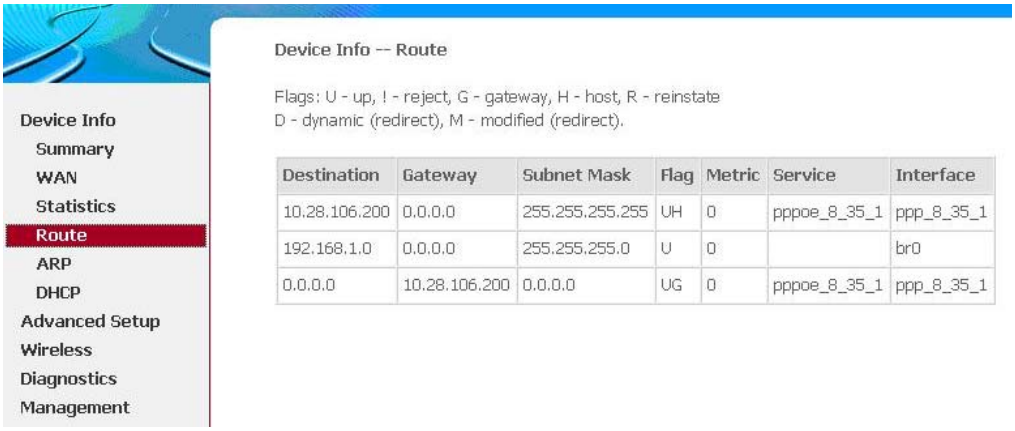


Figure 2.3.8 route table

4.3.9 ARP table information

Click “ARP” to show the following interface. You can query the MAC and IP addresses information of the equipment attached to the MODEM.
Each arp item has information as below:
. IP address
. Flags
. HW address

. Device

Figure 2.3.9 ARP table

4.3.10 DHCP IP Leases information

Click “DHCP” to show the following interface. You can query the IP addresses assignment to which MAC Address in DSL router’s LAN side,Through Ethernet and Wireless can obtain the IP Address from the DHCP server on DSL router.

Each Leases item include info as below:

. Hostname

. MAC Address

. IP Address

. Expires In :How many times the Device Leases the IP Address for the MAC Address

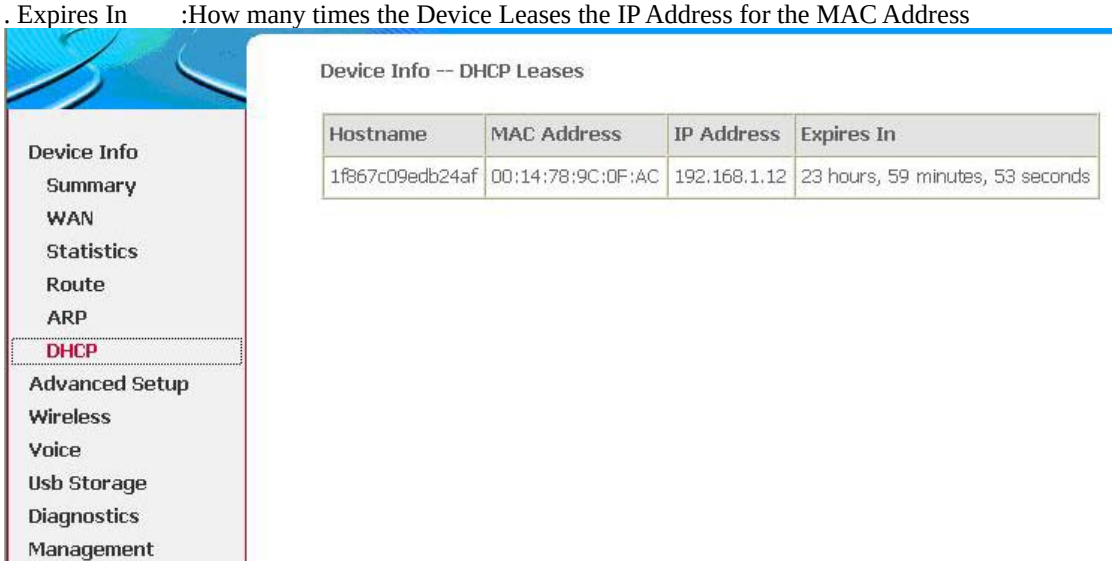


Figure 2.3.10 DHCP Leases List

4.4 Advanced Setup

Click “Advanced Setup” to enter the advanced system setup interface.there many items as below:

. WAN :Wide area network interface,

. LAN :Local area network interface

. NAT :Network Address Translate

. Security

. Quality of Service

. Routing

. DNS :

. DSL

. Print Server

. Port Papping
. IPSec
. Certificate
Advance Setup is DSL Router's config center,

Figure 2.4 Advance Setup menu

4.4.1 WAN CONFIGRATION

Click "Advance Setup"→ "WAN" , there maybe two circumstances appears.
In this Interface you can do:

. Add
. Edit
. Remove
. Save/Reboot

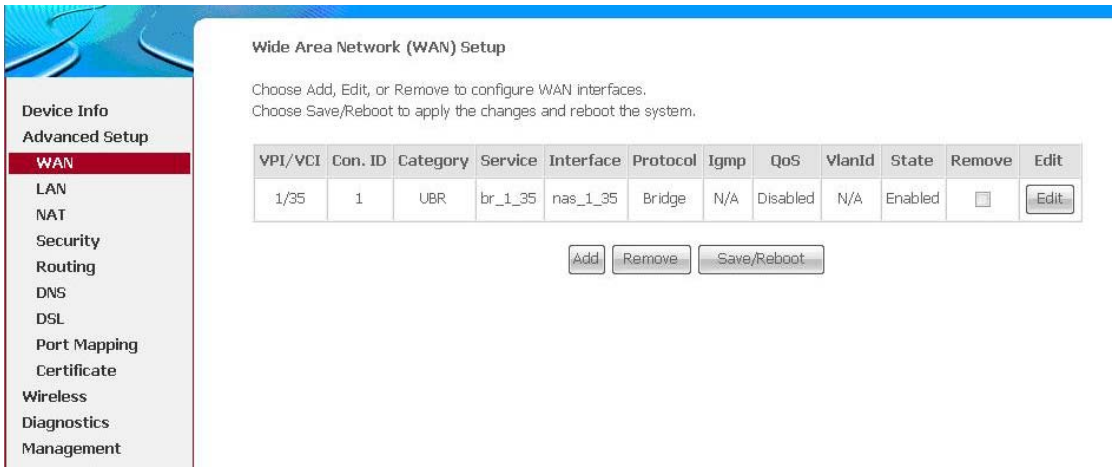


Figure 2.4.1 WAN Config

Select "Add", then it will turn into the following configure screen.
ADD PVC
VLAN OF PVC
Quality Of Service PVC
Service category
ADD PPPoE PVC
PPP IP extension
ADD PPPOA PVC

ADD MER PVC
ADD BRIDGE PVC
ADD IPOA PVC

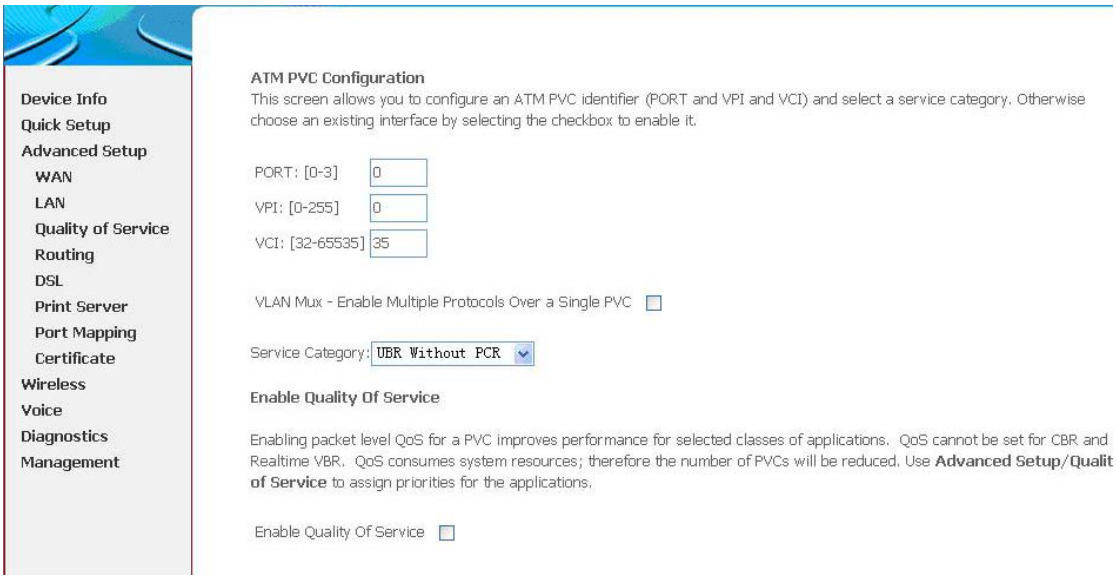

Device Info
Quick Setup
Advanced Setup
WAN
LAN
Quality of Service
Routing
DSL
Print Server
Port Mapping
Certificate
Wireless
Voice
Diagnostics
Management
ATM PVC Configuration
This screen allows you to configure an ATM PVC identifier (PORT and VPI and VCI) and select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.
PORT: [0-3] 0
VPI: [0-255] 0
VCI: [32-65535] 35
VLAN Mux - Enable Multiple Protocols Over a Single PVC
Service Category: UBR Without PCR
Enable Quality Of Service
Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use Advanced Setup/Qualit of Service to assign priorities for the applications.
Enable Quality Of Service

Figure 2.4.2: PVC and it's Qos config page

Look at this screen, is it familiar with us? yeah! It is the same as "Quick Setup", to learn more about the configuration, please turn to page 31.
Have configured the modem
If we have configured the modem, click "WAN" will turn into the following interface:

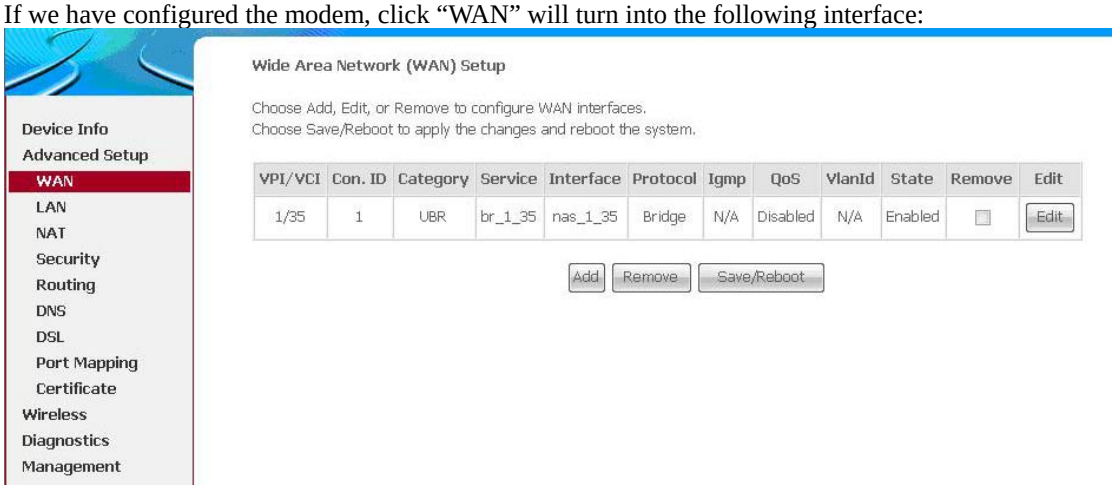


Figure 2.4.3:PPPoE Config

1. Select "Edit", you can modify the existent PVC's parameter;
2. Select "Add", you can add a more one ATM PVC,
3. Choose "Remove", you can delete the PVC(don't forget select the "Remove check box);
4. Select "Save/Reboot", Choose "Save/Reboot" to apply the changes and reboot the system.

Note: After a PVC is deleted or modified, the system must be rebooted, or the modification will not be effective.
Now we only show you how to add PVC.

4.4.1.1 Add PPPoE PVC

Click "Add" to add a certain piece of PVC. The following descriptions are given by an example of adding "PVC 8/35" (PPPOE mode).

1. Click “Add” to turn into the following interface. In this interface, you can modify VPI/VCI, service categories and Qos.

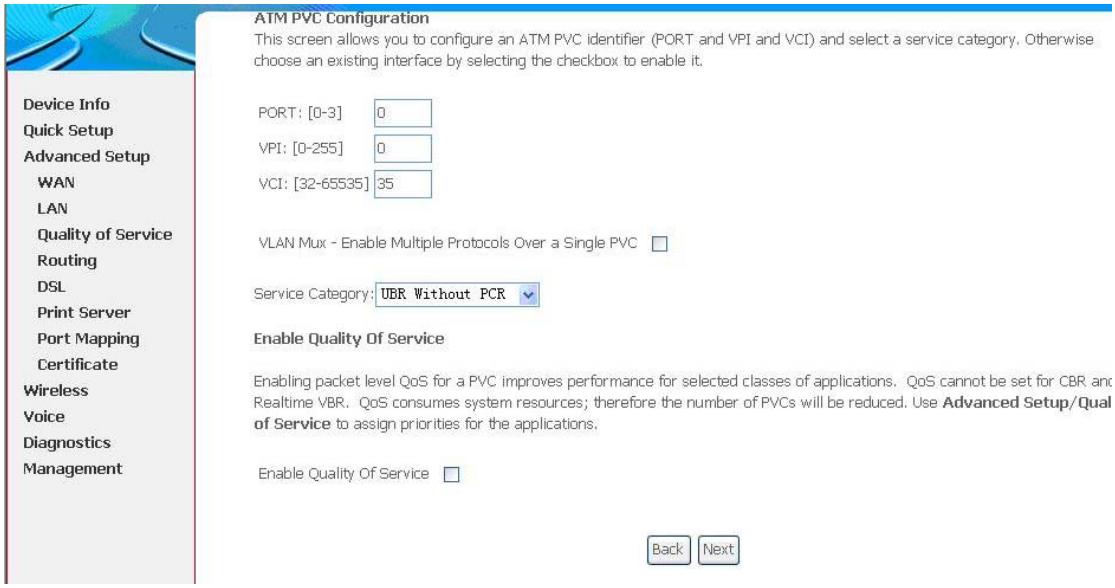

ATM PVC Configuration
This screen allows you to configure an ATM PVC identifier (PORT and VPI and VCI) and select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.
Device Info
Quick Setup
Advanced Setup
WAN
LAN
Quality of Service
Routing
DSL
Print Server
Port Mapping
Certificate
Wireless
Voice
Diagnostics
Management
PORT: [0-3] 0
VPI: [0-255] 0
VCI: [32-65535] 35
VLAN Mux - Enable Multiple Protocols Over a Single PVC
Service Category: UBR Without PCR
Enable Quality Of Service
Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use Advanced Setup/Quality of Service to assign priorities for the applications.
Enable Quality Of Service
Back
Next

Figure 2.4.4: PVC and it’s Qos config page

- **VPI (Virtual Path Identifier)**: The virtual path between two points in an ATM network, and its valid value is from 0 to 255.
- **VCI (Virtual Channel Identifier)**: The virtual channel between two points in an ATM network, ranging from 32 to 65535 (1 to 31 are reserved for known protocols).
- **Service Category:** UBR Without PCR/UBR With PCR/CBR/Non Realtime VBR/Realtime VBR.
- **Enable Quality Of Service:** enable/disable.

In this example, PVC 8/35 is required to modify, so service category and QoS will remain default values. In actual applications, you can modify them depending on your practices.

After proper modifications, click “Next” to show the following interface.

2. In this interface, you can modify Internet Connection Type and Encapsulation Type.

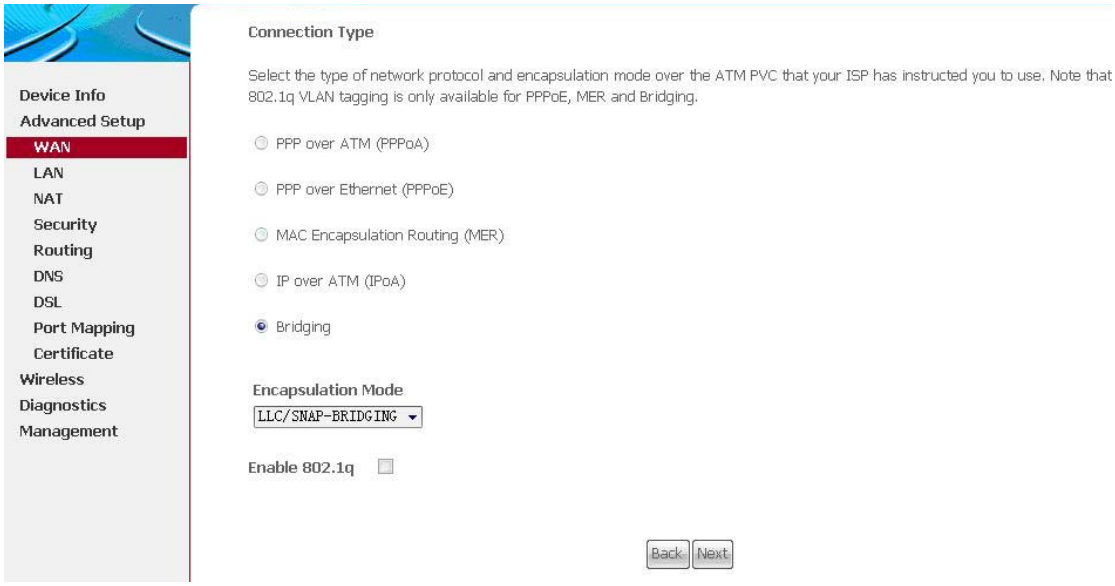


Figure 2.4.5: Internet Connection Type and Encapsulation Type page

Change the connection type of PVC 8/35 to “PPP over ATM (PPPoE)”.
Select “PPP over ATM (PPPoE)”, and “LLC/SNAP-BRIDGING” (depending on the uplink equipment,

generally “LLC/SNAP-BRIDGING”) as “Encapsulation Mode”.

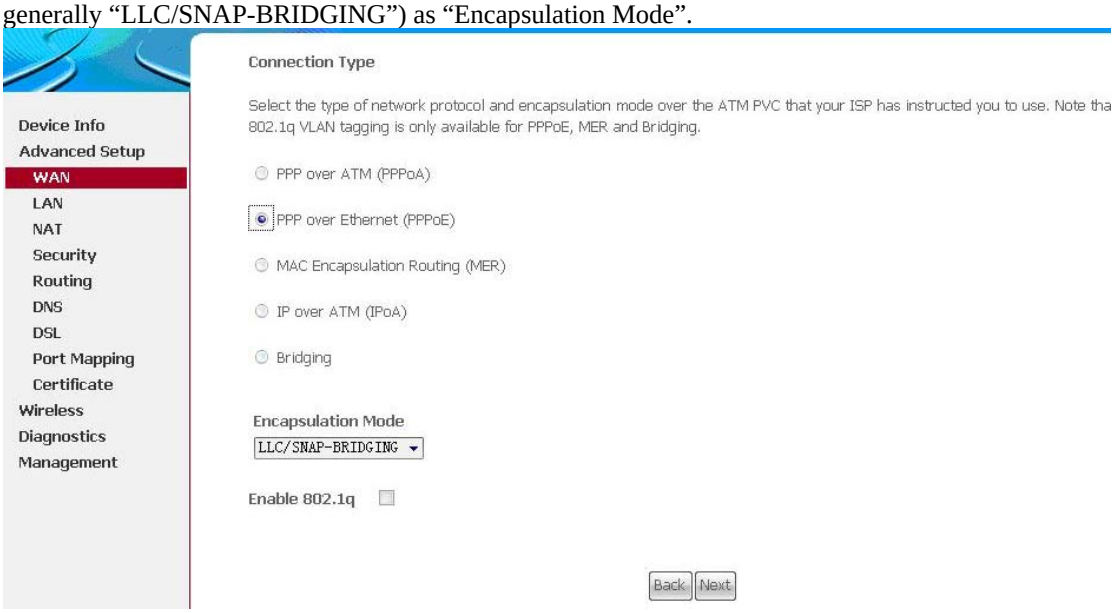


Figure 2.4.6:PPP over Ethernet(PPPoE)

Enable 802.1q: If enable it, input the 802.1q VLAN tag value. Note that 802.1q VLAN tagging is only available for PPPoE, MER and Bridge.

Click “Next” to show the following interface.

3. In this interface, you can modify the PPP Username, PPP Password, Authentication Method and so on.

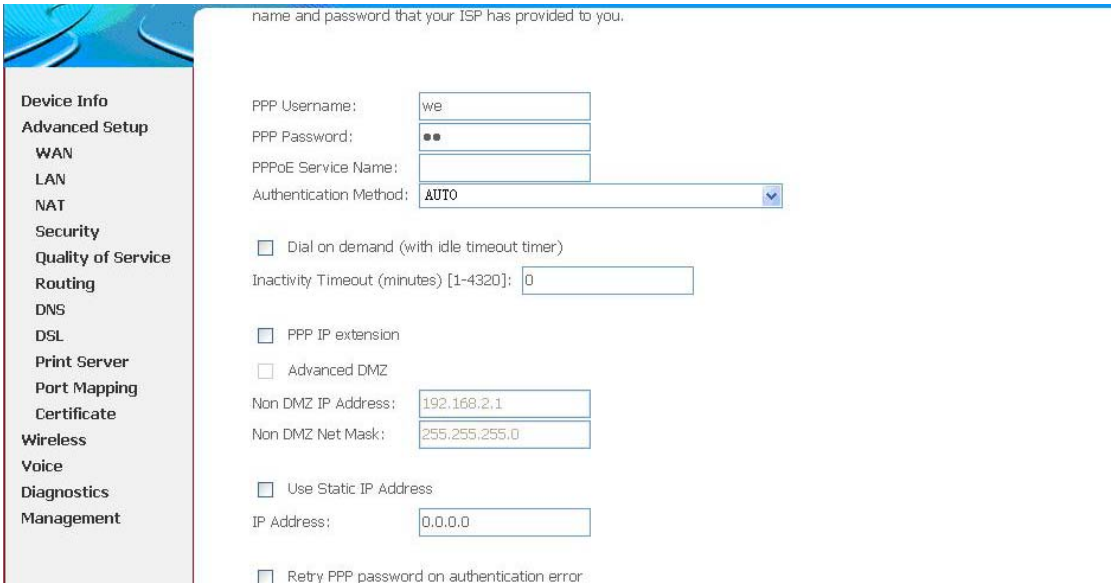


Figure 2.4.7: PPP information and others funtion page

PPP Username: the correct user name that your ISP has provided to you.

PPP Password: the correct password that your ISP has provided to you.

PPPoE Service Name: If your ISP provided it to you, please input it. Unless don’t input anything.

Authentication Method: AUTO, PAP, CHAP, MSCHAP. Usually select AUTO will be OK.

Dial on demand (with idle timeout timer): If enable it, you need to input the idle timeout time. Within the preset minutes, if the MODEM doesn’t detect the flow of the user continuously, the MODEM will automatically disconnect the PPPOE connection. Once it detects the flow (like access to a webpage), the MODEM will restart the PPPOE dial up.

If disable it, the MODEM will perform PPPOE dial-up all the time. Unless the MODEM is powered off and DSLAM or uplink equipment are abnormal, the PPPOE connnection will not broken.

PPP IP extension: After "PPP IP extension" is enabled, the WAN IP address obtained by the MODEM through built-in dial-up can be directly assigned to the PC being attached with the MODEM (at this time, the MODEM has only one PC). From the view of the PC user, this is even with that the PC dials up to obtain an IP addres. But actually, the dial-up is done by the MODEM.

If disable it, the MODEM obtain the WAN IP address itself.

Advanced DMZ: This is the virtual server configuration option. The DMZ Host feature allows one local computer to be exposed to the internet, to be this feature,the other computer can easily enter the DMZ Host, a DMZ host is not protected by the firewall and may be vulnerable to attack. Designating a DMZ host may also put other computers in the home network at risk. When designating a DMZ host, you must consider the security implications and protect it if necessary.

1. If you want to setup DMZ Host, you should enable the "PPP IP extension" at first;
2. **Non DMZ IP Address:** The DMZ Host IP Address, you can modify it by hand;
3. **Non DMZ Net Mask:** The DMZ Host Subnet Mask, it is build upon the DMZ Host IP Address.

Use Static IP Address: If disabled it, the MODEM through PPPOE dial-up, to obtain an IP address assigned by an uplink equipment such as BAS.

If enable it, the MODEM use this IP as the WAN IP address.

After input the PPP Username and PPP Password, click "Next" to show the following interface.

- In this interface, you can modify the Service name and enable/disable the IGMP Multicast, WAN Service.

Figure 2.4.8: PPPoE IGMP and WAN service page

IGMP Multicast: IGMP proxy. For example, if you need PPPoE mode support IPTV, please enable it.

WAN Service: Please enable it, unless you don't need to active the PVC.

Click "Next" to show the following interface.

- In this interface, it show the all configuration. You can see some default values: NAT enable, Firewall enable.

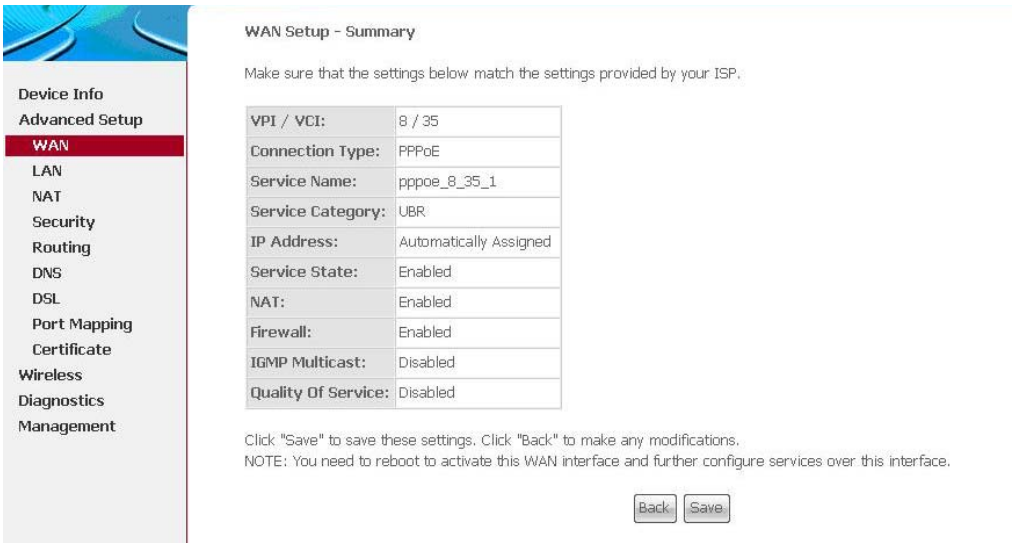


Figure 2.4.9:PPPoE Setup Summary

Click “Save” to save these settings.And you can click “Back” to make any modifications. After you click “Save”, it show the following interface.

NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

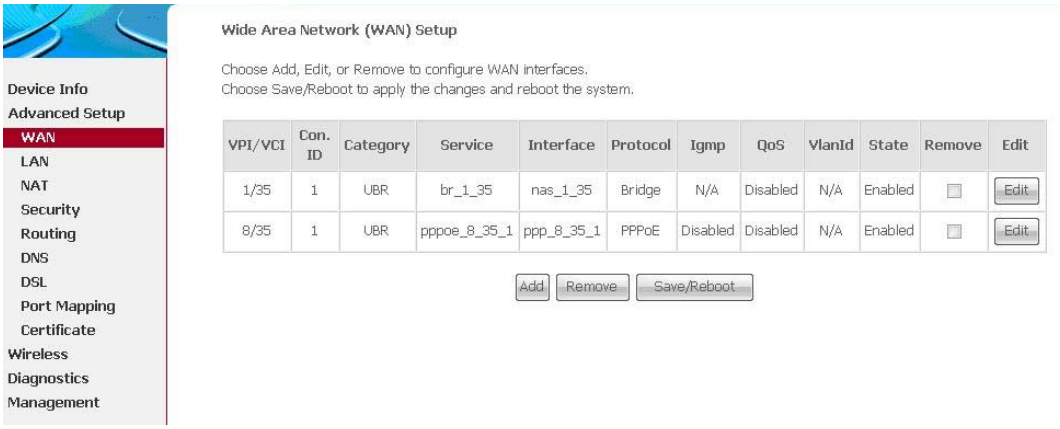
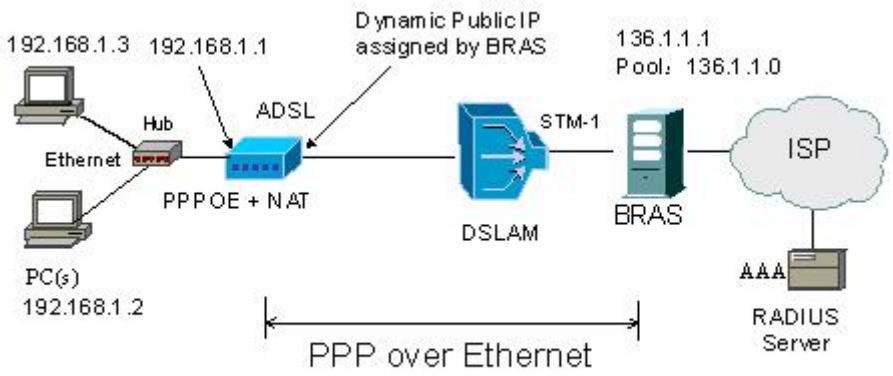


Figure 2.4.10:PPPoE Setup Complete

4.4.1.2 PPPoE PVC Network Application



Descriptions

In this example, the MODEM is connected to the DSLAM through PVC 8/35 and the access mode is the built-in PPPOE+NAT. The encapsulation of the BRAS downlink port is PPP OVER ETHERNET, the authentication is AUTO, the IP address is 10.28.106.200, the IP Pool is 10.28.106.*, and the IP address of uplink port is 10.61.92.157. The IP of the WAN port on the MODEM is assigned by BRAS through the built-in PPPOE dial-up dynamically. The PC that the MODEM is attached is assigned with a private IP address (within the same segment with the management IP of the MODEM). The NAT functions of the MODEM will be enabled and the private PC address will be translated to the public address 10.28.106.* (2 ~ 254) assigned by BRAS dynamically for accessing ISP.
The IP address of the PC can be fixed (as in this example) or assigned through DHCP Server of the MODEM. If it is assigned by DHCP Server, the DHCP functions of the MODEM must be enabled. The IP address of the DHCP address pool is 192.168.1.* (2~254). The functions are enabled by default and at the same time the PC is configured to obtain IP and DNS addresses dynamically.

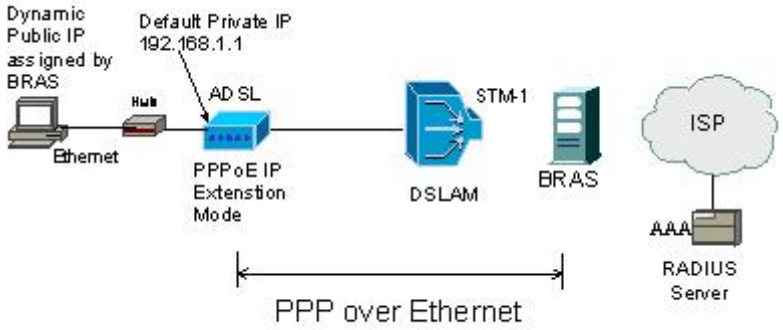
Setting

1. Activate your browser and input "192.168.1.1" in the address column to login the MODEM.
2. Click "**Advanced Setup**" -> "**WAN**", then click "add".
3. In the "**ATM PVC Configuration"** interface configure VPI/VCI as 8/35 and then click "Next".
4. In the "**Connection Type**" interface, select "PPP over Ethernet (PPPoE)" and "LLC/SNAP-BRIDGING" as the encapsulation, and then click "Next".
5. In the "**PPP User name and Password**" interface, enter the user name and password provided by your ISP. And then click "Next".
6. In the "**Enable IGMP Multicast, and WAN Service**" interface, keep the default configuration unchanged and then click "Next".
7. Check the network configurations and make sure that all settings agree with the data provided by your ISP, and then click "Save".
8. Click "Save/Reboot" to apply the changes and reboot the system.

You can also modify the PVC 8/35. If you need to modify the LAN IP address and DHCP server information, you can do it in "LAN" in "Advanced Setup".
After the dial-up is successful, the IP address that the MODEM obtains at the WAN-side port ppp_8_35_1. Query "Device Info"→ "Route" and the route table is as follows:

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
10.28.106.200	0.0.0.0	255.255.255.255	UH	0	pppoe_8_35_1	ppp_8_35_1
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0
0.0.0.0	10.28.106.200	0.0.0.0	UG	0	pppoe_8_35_1	ppp_8_35_1

4.4.1.3 PPPoE PVC IP Extension Mode



Descriptions

In this example, the MODEM is connected to the DSLAM through "PVC 8/35"; the PPPOE is located between the WAN interface of the MODEM and BRAS. The encapsulation of the downlink interface of BRAS is "PPP OVER ETHERNET", the authentication is AUTO, the IP address is 10.28.106.200, the

IP Pool is 10.28.106.*, and the IP address of the uplink interface is 10.61.92.157.
The WAN interface of the MODEM obtains the IP address that is dynamically assigned by BRAS through its built-in PPPOE dial-up. The MODEM will assign this public IP address to the PC (configured as "Obtain an IP address automatically") attached to it in the DHCP mode. At this time, NAT will have no effect. From the point view of the user, the MODEM seems working in the "Briding" mode.
In some cases, this function is named ZIPB (Zero Installation PPP Bridge Mode) as well.
Setting

1. Activate your browser and input "192.168.1.1" in the address column to login the MODEM.
2. Click "**Advanced Setup**" -> "**WAN**", then click "add".
3. In the "**ATM PVC Configuration"** interface configure VPI/VCI as 8/35 and then click "Next".
4. In the "**Connection Type**" interface, select "PPP over Ethernet (PPPoE)" and "LLC/SNAP-BRIDGING" as the encapsulation, and then click "Next".
5. In the "**PPP User name and Password**" interface, enter the user name and password provided by your ISP.

   IMPORTENT: Select "Enable PPP IP extension".

   And then click "Next".
6. In the "**Enable IGMP Multicast, and WAN Service**" interface, keep the default configuration unchanged and then click "Next".
7. Check the network configurations and make sure that all settings agree with the data provided by your ISP, and then click "Save".
8. Click "Save/Reboot" to apply the changes and reboot the system.

If you need to modify the LAN IP address, you can do it in "LAN" of "Advance".
After the PPPOE dialup which is built in the MODEM is successful, the IP address 10.28.106.82 is obtained. Enter "Device Info" → "WAN". Show below:

Figure 2.5.1:WAN PPPoE Info

4.4.1.4 Add PPPoA PVC

Click "Add" to add a certain piece of PVC. The following descriptions are given by an example of adding "PVC 8/35" (PPPOA mode).

- Click "Add" following "PVC 8/35".

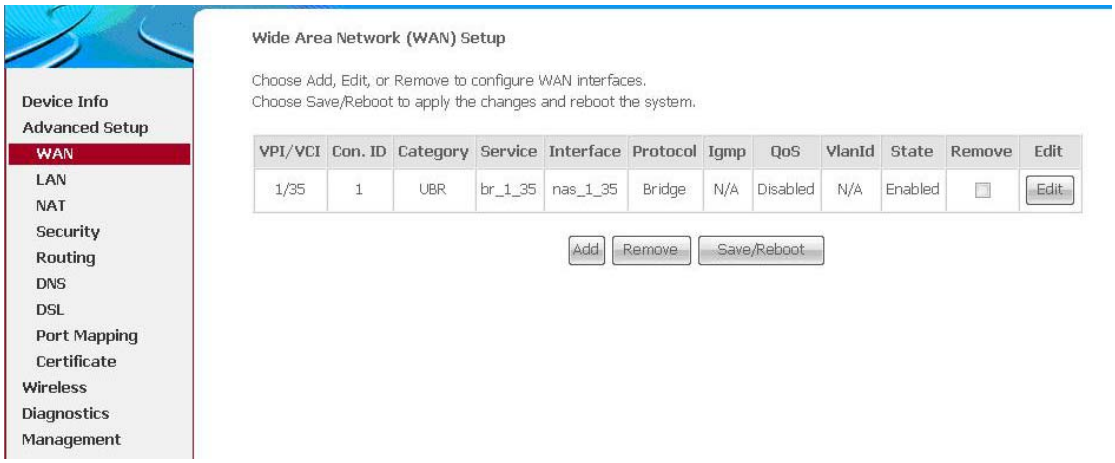


Figure 2.5.2:PPPoA Config

- In this interface, you can modify VPI/VCIs, service categories and QoS.

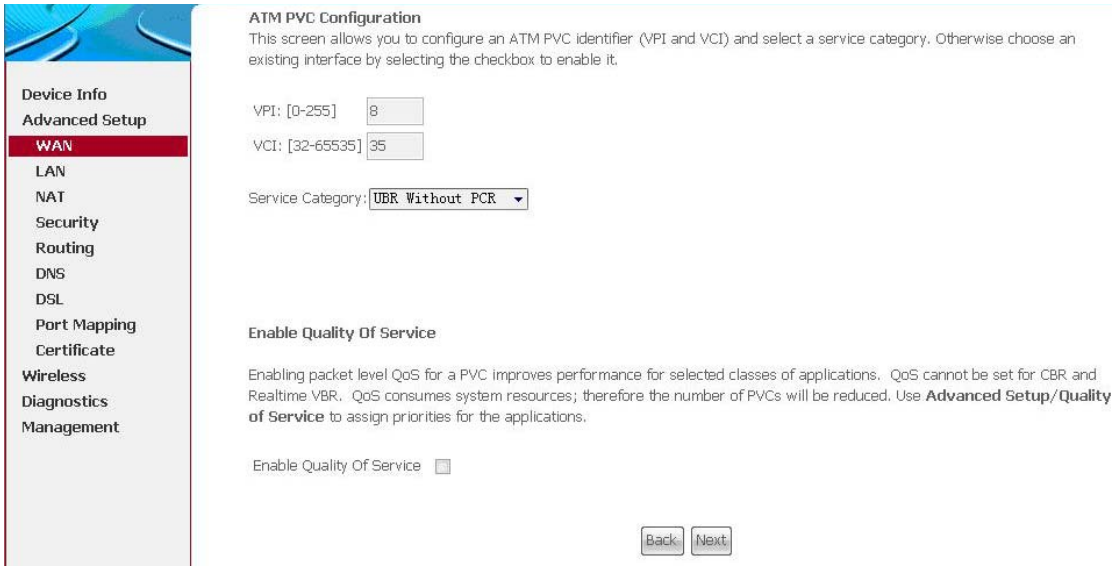

Device Info
Advanced Setup
WAN
LAN
NAT
Security
Routing
DNS
DSL
Port Mapping
Certificate
Wireless
Diagnostics
Management
ATM PVC Configuration
This screen allows you to configure an ATM PVC identifier (VPI and VCI) and select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.
VPI: [0-255] 8
VCI: [32-65535] 35
Service Category: UBR Without PCR
Enable Quality Of Service
Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use Advanced Setup/Quality of Service to assign priorities for the applications.
Enable Quality Of Service
Back Next

Figure 2.5.3: PVC and it's Qos config page

VPI (Virtual Path Identifier): The virtual path between two points in an ATM network, and its valid value is from 0 to 255.

VCI (Virtual Channel Identifier): The virtual channel between two points in an ATM network, ranging from 32 to 65535 (1 to 31 are reserved for known protocols).

Service Category: UBR Without PCR/UBR With PCR/CBR/Non Realtime VBR/Realtime VBR.

Enable Quality Of Service: enable/disable.

In this example, PVC 8/35 is required to modify, so service category and QoS will remain default values. In actual applications, you can modify them depending on your practices.

After proper modifications, click "Next" to show the following interface.

- In this interface, you can modify Internet Connection Type and Encapsulation Type.

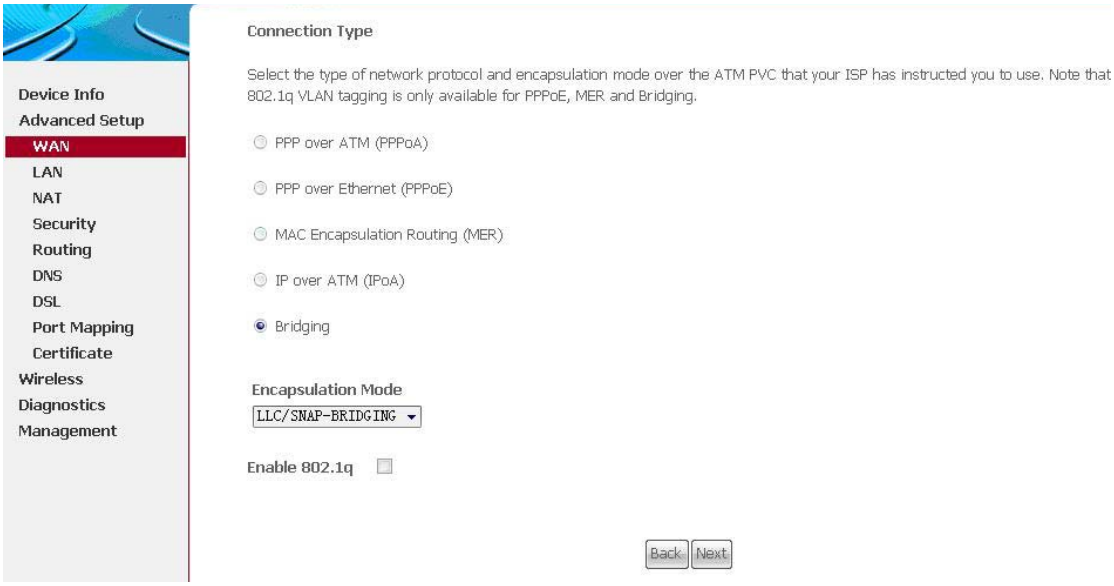


Figure 2.5.4: Internet Connection Type and Encapsulation Type page

Change the connection type of PVC 8/35 to “PPP over ATM (PPPoA)”.

Select “PPP over ATM (PPPoA)”, and “VC/MUX” (depending on the uplink equipment, generally “VC/MUX”) as “Encapsulation Mode”.

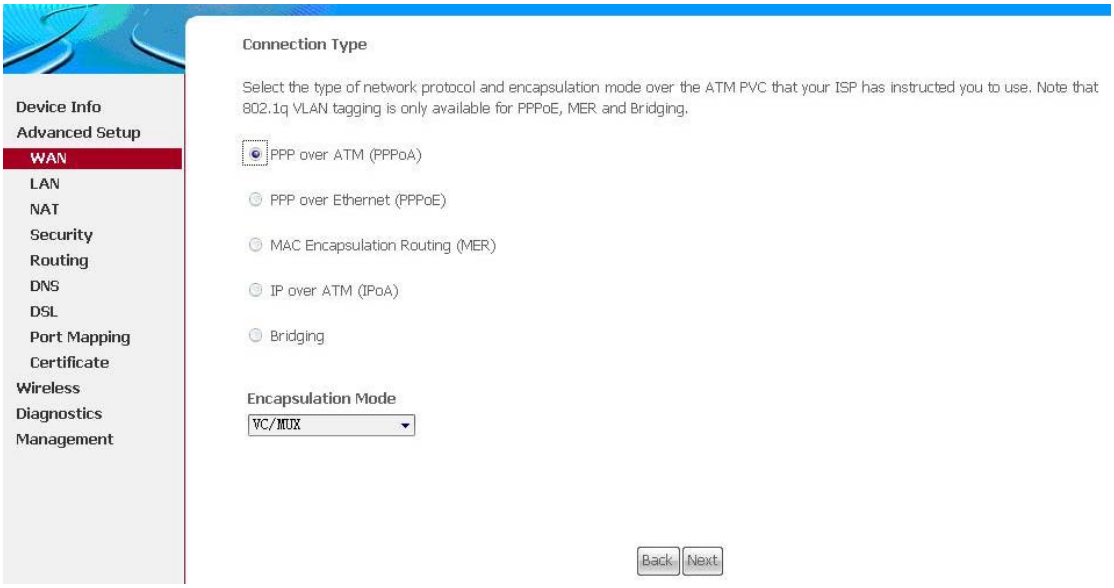


Figure 2.5.5:PPP over ATM(PPPoA)

Click “Next” to show the following interface.

- In this interface, you can modify the PPP Username, PPP Password, Authentication Method and so on.

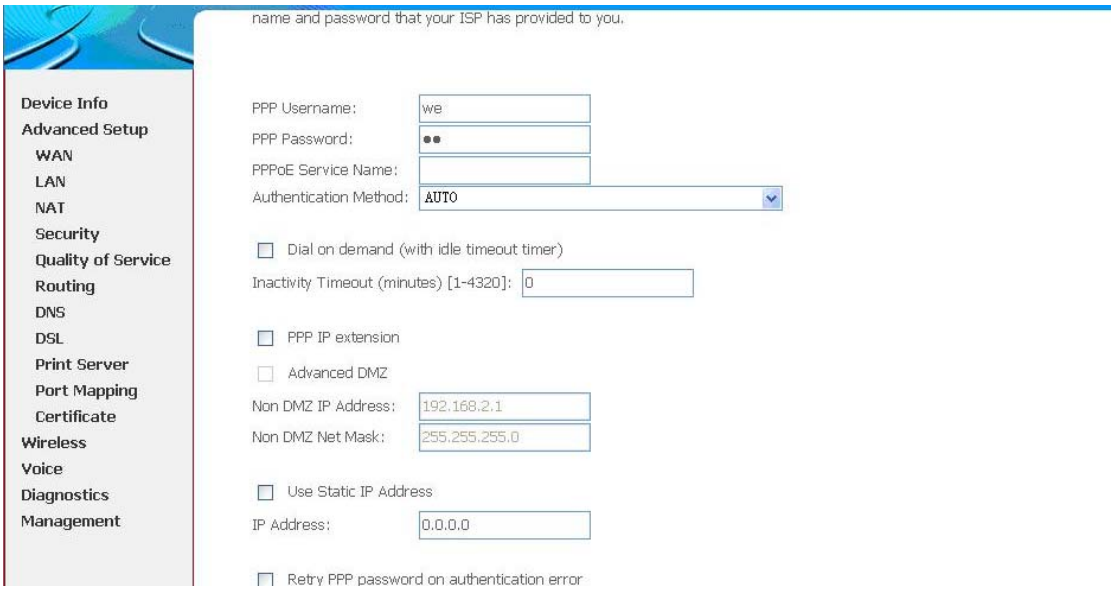


Figure 2.5.6: PPP information and others funtion page

PPP Username: the correct user name that your ISP has provided to you.

PPP Password: the correct password that your ISP has provided to you.

Authentication Method: AUTO, PAP, CHAP, MSCHAP. Usually select AUTO will be OK.

Dial on demand (with idle timeout timer): If enable it, you need to input the idle timeout time. Within the preset minutes, if the MODEM doesn't detect the flow of the user continuously, the MODEM will automatically disconnect the PPPOA connection. Once it detects the flow (like access to a webpage), the MODEM will restart the PPPOA dial up.

If disable it, the MODEM will perform PPPOA dial-up all the time. Unless the MODEM is powered off and DSLAM or uplink equipment are abnormal, the PPPOA connnection will not broken.

PPP IP extension: After "PPP IP extension" is enabled, the WAN IP address obtained by the MODEM through built-in dial-up can be directly assigned to the PC being attached with the MODEM (at this time, the MODEM has only one PC). From the view of the PC user, this is even with that the PC dials up to obtain an IP addres. But actually, the dial-up is done by the MODEM.

If disable it, the MODEM obtain the WAN IP address itself.

Advanced DMZ: This is the virtual server configuration option. The DMZ Host feature allows one local computer to be exposed to the internet, to be this feature,the other computer can easily enter the DMZ Host, a DMZ host is not protected by the firewall and may be vulnerable to attack. Designating a DMZ host may also put other computers in the home network at risk. When designating a DMZ host, you must consider the security implications and protect it if necessary.

1. If you want to setup DMZ Host, you should enable the "PPP IP extension" at first;
2. **Non DMZ IP Address:** The DMZ Host IP Address, you can modify it by hand;
3. **Non DMZ Net Mask:** The DMZ Host Subnet Mask, it is build upon the DMZ Host IP Address.

Use Static IP Address: If disabled it, the MODEM through PPPOA dial-up, to obtain an IP address assigned by an uplink equipment such as BAS.

If enable it, the MODEM use this IP as the WAN IP address.

After input the PPP Username and PPP Password, click "Next" to show the following interface.

- In this interface, you can modify the Service name and enable/disable the IGMP Multicast, WAN Service.

Figure 2.5.6: PPPoA IGMP and WAN service page

IGMP Multicast: IGMP proxy. For example, if you need PPPoA mode support IPTV, please enable it.
WAN Service: Please enable it, unless you don't need to active the PVC.
Click "Next" to show the following interface.

- In this interface, it show the all configuration. You can see some default values: NAT enable, Firewall enable.

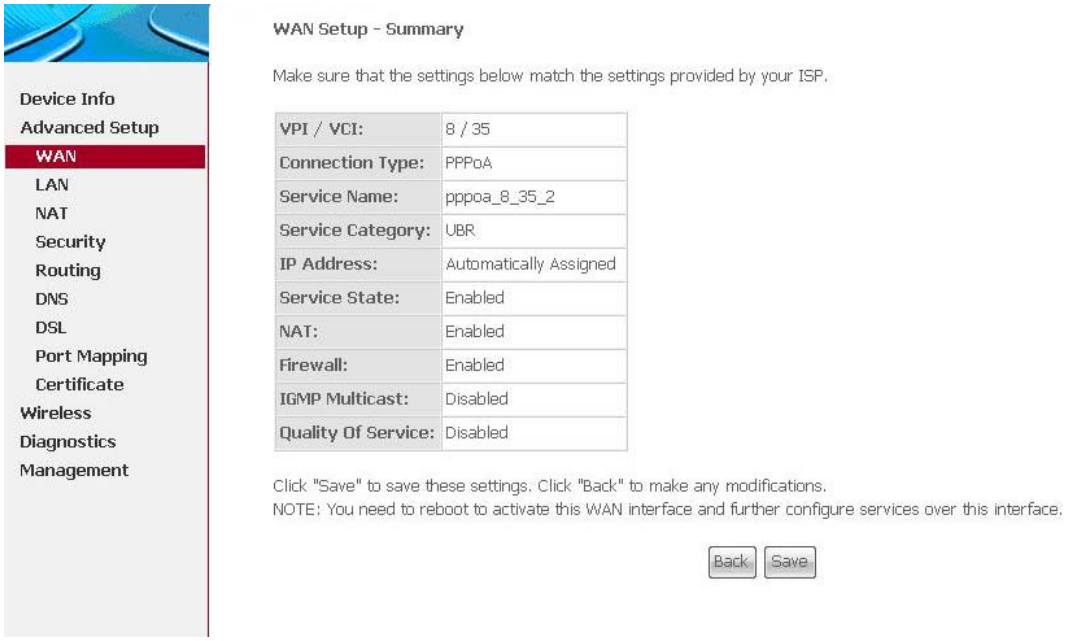


Figure 2.5.7:PPPoA Setup Summary

Click "Save" to save these settings.And you can click "Back" to make any modifications. After you click "Save", it show the following interface.
NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

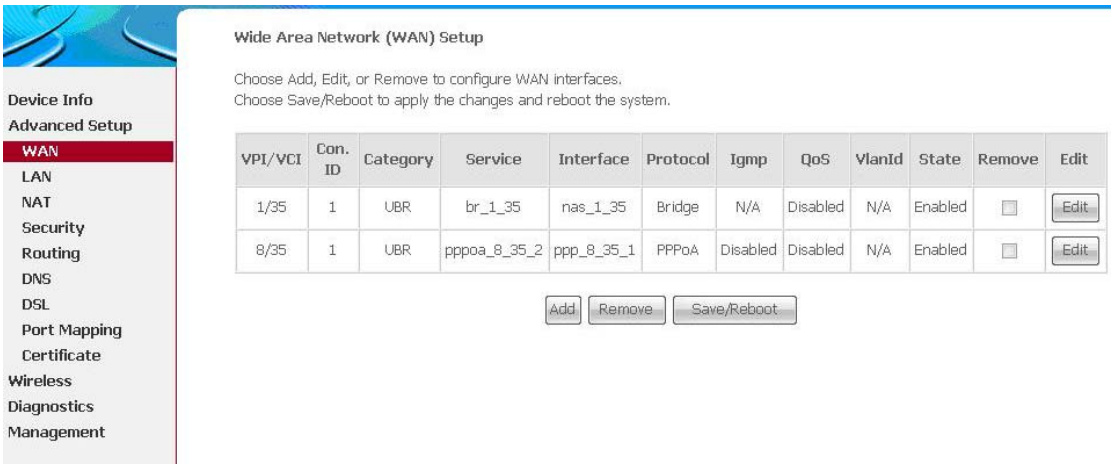
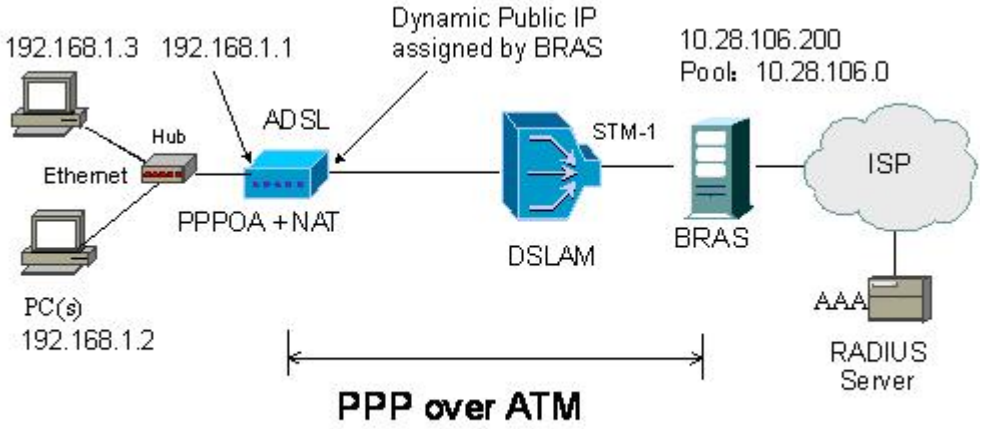


Figure 2.5.8:PPPoA Setup Complete

4.4.1.5 PPPoA PVC Network Application



Descriptions

In this example, the MODEM is connected to the DSLAM through PVC 8/35 and the access mode is the built-in PPPOA+NAT. The encapsulation of the BRAS downlink port is PPP OVER ATM, the authentication is AUTO, the IP address is 10.28.106.200, the IP Pool is 10.28.106.*, and the IP address of uplink port is 10.61.92.157. The IP of the WAN port on the MODEM is assigned by BRAS through the built-in PPPOA dial-up dynamically. The PC that the MODEM is attached is assigned with a private IP address (within the same segment with the management IP of the MODEM). The NAT functions of the MODEM will be enabled and the private PC address will be translated to the public address 10.28.106.* (2 ~ 254) assigned by BRAS dynamically for accessing ISP.

The IP address of the PC can be fixed (as in this example) or assigned through DHCP Server of the MODEM. If it is assigned by DHCP Server, the DHCP functions of the MODEM must be enabled. The IP address of the DHCP address pool is 192.168.1.* (2~254). The functions are enabled by default and at the same time the PC is configured to obtain IP and DNS addresses dynamically.

Setting:

1. Activate your browser and input “192.168.1.1” in the address column to login the MODEM.
2. Click “**Advanced Setup**” -> “**WAN**”, then click “add”.
3. In the “**ATM PVC Configuration”** interface configure VPI/VCI as 8/35 and then click “Next”.
4. In the “**Connection Type**” interface, select “PPP over ATM (PPPoA)” and “VC MUX” as the encapsulation, and then click “Next”.
5. In the “**PPP User name and Password**” interface, enter the user name and password provided by

your ISP. And then click “Next”.

6. In the “**Enable IGMP Multicast, and WAN Service**” interface, keep the default configuration unchanged and then click “Next”.
7. Check the network configurations and make sure that all settings agree with the data provided by your ISP, and then click “Save”.
8. Click “Save/Reboot” to apply the changes and reboot the system.

You can also modify the PVC 8/35. If you need to modify the LAN IP address and DHCP server information, you can do it in “LAN” in “Advanced Setup”.
After the dial-up is successful, the IP address that the MODEM obtains at the WAN-side port ppp_8_35_1. Query “Device Info”→ “Route” and the route table is as follows:

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
10.28.106.200	0.0.0.0	255.255.255.255	UH	0	pppoa_8_35_1	ppp_8_35_1
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0
0.0.0.0	10.28.106.200	0.0.0.0	UG	0	pppoa_8_35_1	ppp_8_35_1

Note: After the built-in PPPOA dial-up is successful, the created WAN-side port is ppp_8_35_1.

4.4.1.6 Add MER PVC

Click “Add” to add a certain piece of PVC. The following descriptions are given by an example of adding “PVC 8/35” (MER mode).

- Click “Add” following “PVC 8/35”.

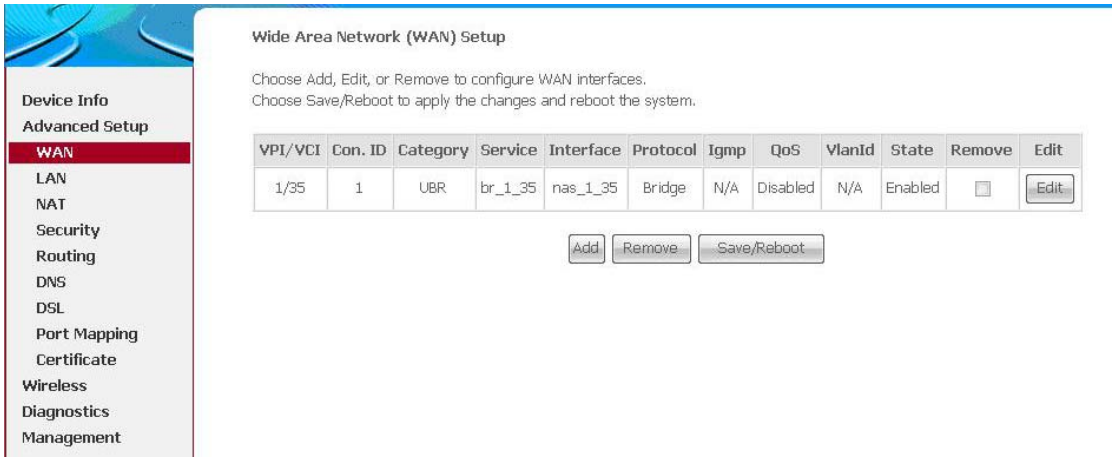


Figure 2.5.9:MER Config

- In this interface, you can modify VPI/VCIs, service categories and QoS.

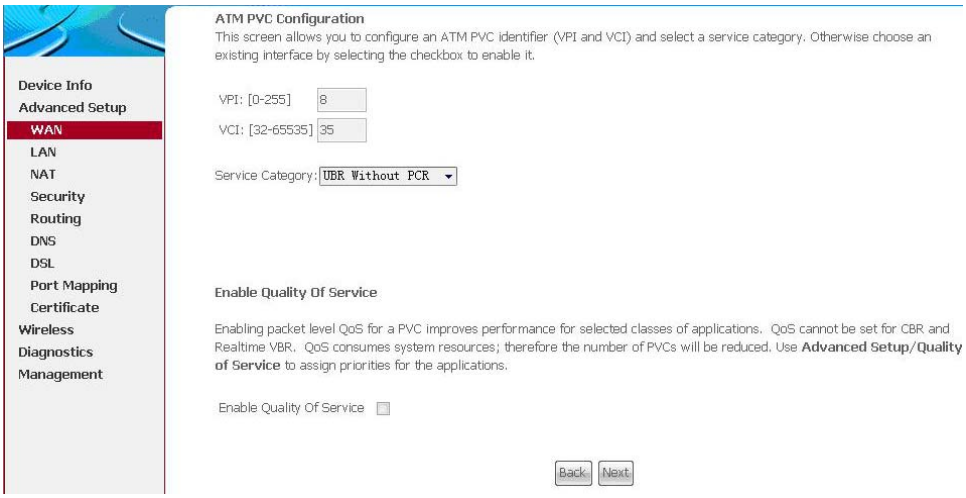

ATM PVC Configuration
This screen allows you to configure an ATM PVC identifier (VPI and VCI) and select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Routing
DNS
DSL
Port Mapping
Certificate
Wireless
Diagnostics
Management
VPI: [0-255] 8
VCI: [32-65535] 35
Service Category: UBR Without PCR
Enable Quality Of Service
Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use Advanced Setup/Quality of Service to assign priorities for the applications.
Enable Quality Of Service
Back
Next

Figure 2.5.10: PVC and it's Qos config page

VPI (Virtual Path Identifier): The virtual path between two points in an ATM network, and its valid value is from 0 to 255.

VCI (Virtual Channel Identifier): The virtual channel between two points in an ATM network, ranging from 32 to 65535 (1 to 31 are reserved for known protocols).

Service Category: UBR Without PCR/UBR With PCR/CBR/Non Realtime VBR/Realtime VBR.

Enable Quality Of Service: enable/disable.

In this example, PVC 8/35 is required to modify, so service category and QoS will remain default values. In actual applications, you can modify them depending on your practices.

After proper modifications, click "Next" to show the following interface.

- In this interface, you can modify Internet Connection Type and Encapsulation Type.

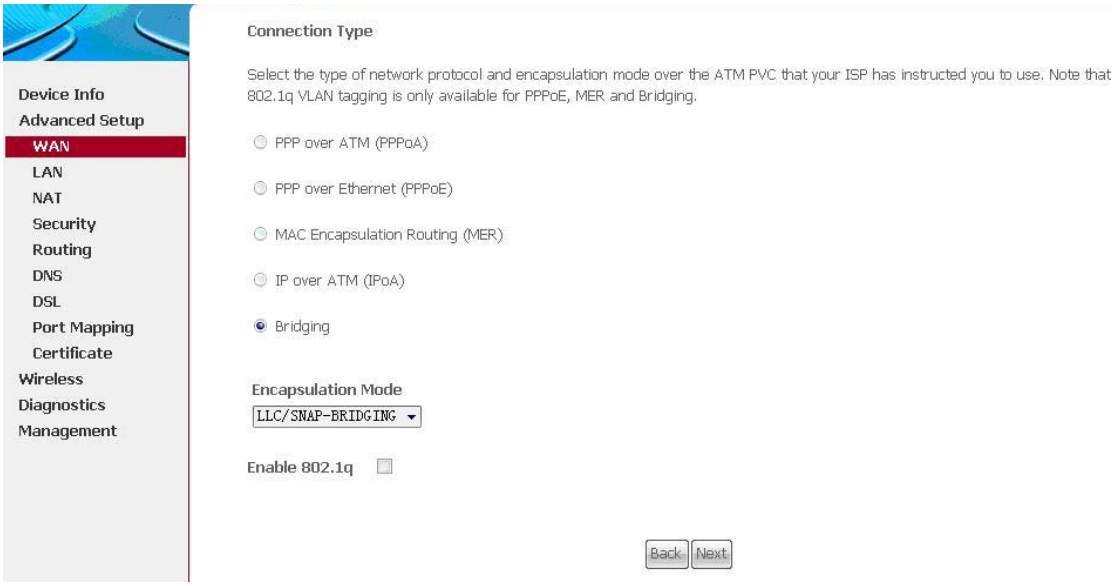


Figure 2.6.1: Internet Connection Type and Encapsulation Type page

Change the connection type of PVC 8/35 to "MAC Encapsulation Routing (MER)".

Select "MAC Encapsulation Routing (MER)", and "LLC/SNAP-BRIDGING" (depending on the uplink equipment, generally "LLC/SNAP-BRIDGING") as "Encapsulation Mode".

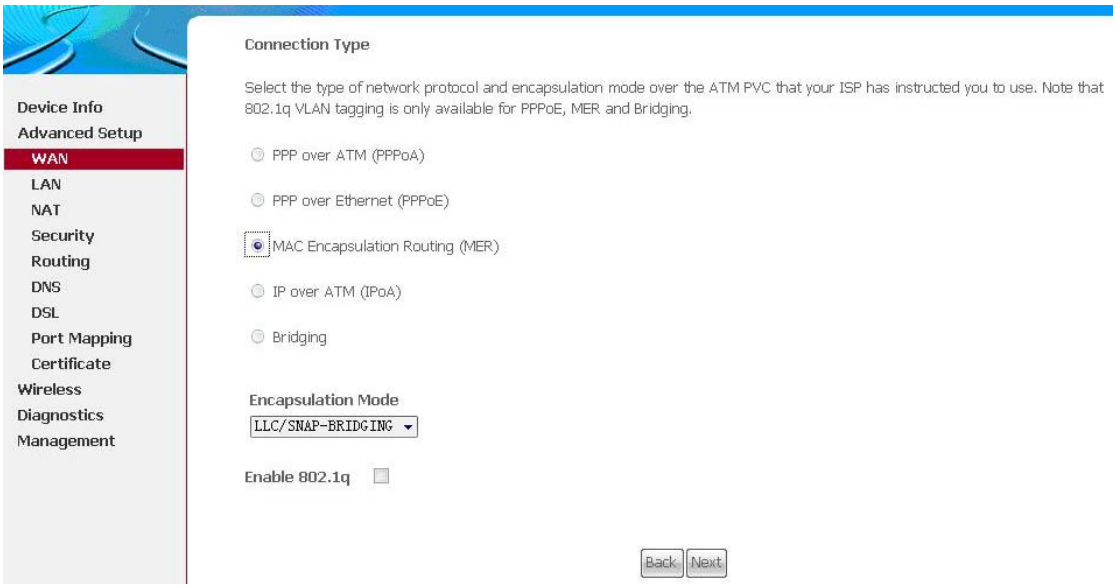


Figure 2.6.2: MAC Encapsulation Routing (MER)

Enable 802.1q: If enable it, input the 802.1q VLAN tag value. Note that 802.1q VLAN tagging is only available for PPPoE, MER and Bridge.

Click “Next” to show the following interface.

- In this interface, you can modify the WAN IP address, Default Gateway and DNS Server settings.

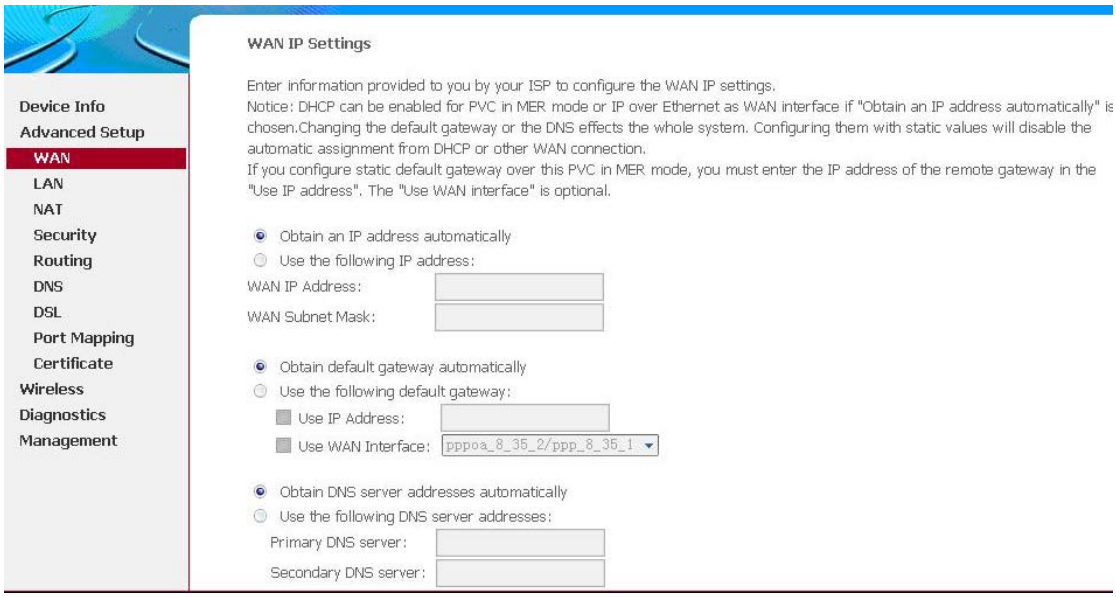

WAN IP Settings
Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: DHCP can be enabled for PVC in MER mode or IP over Ethernet as WAN interface if "Obtain an IP address automatically" is chosen.Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection.
If you configure static default gateway over this PVC in MER mode, you must enter the IP address of the remote gateway in the "Use IP address". The "Use WAN interface" is optional.
Obtain an IP address automatically
Use the following IP address:
WAN IP Address:
WAN Subnet Mask:
Obtain default gateway automatically
Use the following default gateway:
Use IP Address:
Use WAN Interface:
pppoa_8_35_2/ppp_8_35_1
Obtain DNS server addresses automatically
Use the following DNS server addresses:
Primary DNS server:
Secondary DNS server:
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Routing
DNS
DSL
Port Mapping
Certificate
Wireless
Diagnostics
Management

Figure 2.6.3: MER WAN IP config page

Obtain an IP address automatically: The MODEM will obtain a (WAN) IP address automatically and at this time it will enable DHCP Client functions. The WAN IP address is obtained from the uplink equipment like BAS and the uplink equipment is required to enable the DHCP Server functions.

Use the following IP address: If you want to input the WAN ip address by yourself. Check this entry and then input related data in the field.

WAN IP Address: Input the IP address of the WAN interface provided by your ISP.

WAN Subnet Mask: Input the subnet mask concerned to the IP address of the WAN interface provided by your ISP.

Obtain Default Gateway automatically: To obtain the IP address of the default gateway assigned by the uplink equipment such as BAS.

Use the following Default Gateway: If you want to input the IP address of the default gateway by yourself, click this entry and then input related data in the fields.

Use IP Address: Input the gateway of the WAN interface provided by your ISP.

Use WAN Interface: As to BAS equipment, it is the IP address of the downlink interface.

Obtain DNS server address automatically: To obtain the IP address of the DNS server assigned by the uplink equipment such as BAS.
Use the following DNS server addesses: If you want to input the IP address of the DNS server by yourself, click this entry and then input related data in the fields.
Primary DNS server: Input the IP address of the primary DNS server here.
Secondary DNS server: Input the IP address of the secondary DNS server provided by your ISP here.
After correctly modifications, click “Next” to show the following interface.

- In this interface, you can modify the Service name and enable/disable the NAT, Firewal, IGMP Multicast, WAN Service.

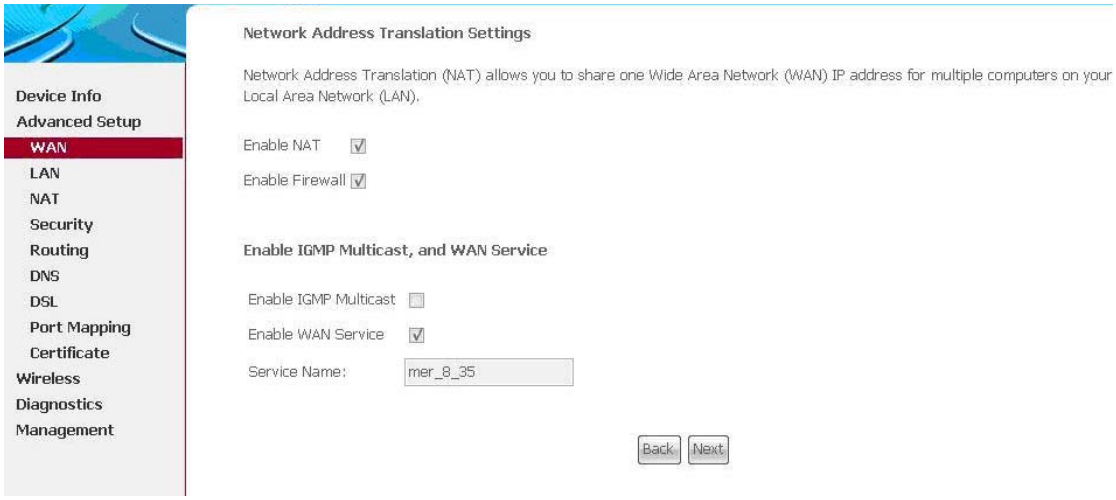


Figure 2.6.4:MER IGMP and WAN service page

Enable NAT: Select it to enable the NAT functions of the MODEM. If you are not to enable NAT and intend the user of the MODEM to access the Internet normally, you must add a route on the uplink equipment; otherwise the access to the Internet will fail. Normally, it is required to enable NAT.
Enable Firewall: enable/disable IP filtering.
IGMP Multicast: IGMP proxy. For example, if you need MER mode support IPTV, please enable it.
WAN Service: Please enable it, unless you don’t need to active the PVC.
Click “Next” to show the following interface.

- In this interface, it show the all configuration.

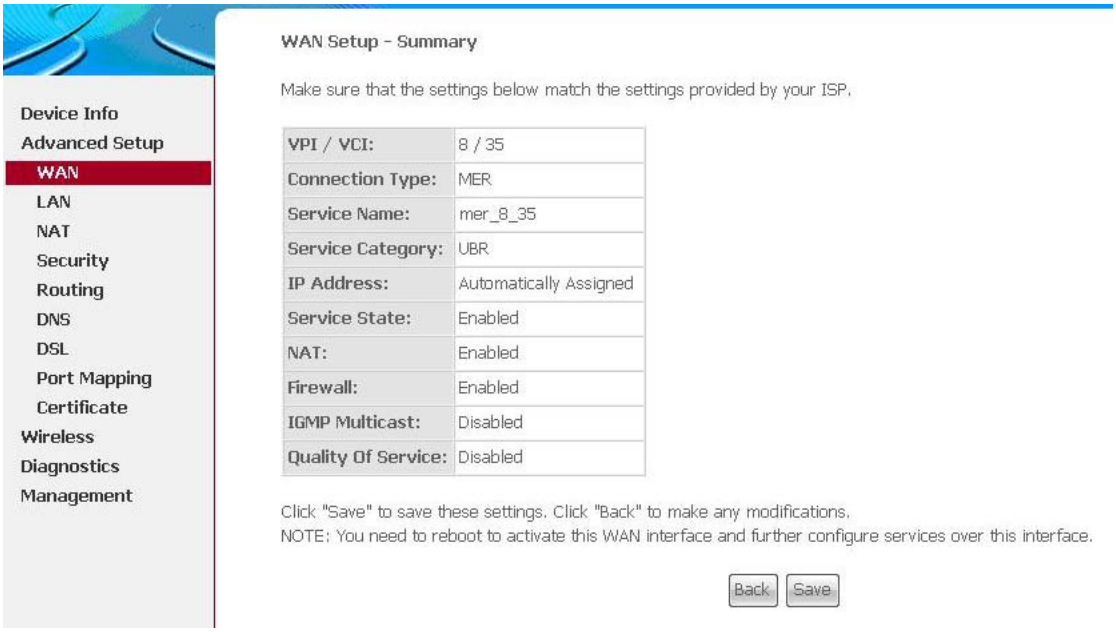


Figure 2.6.5:MER Setup Summary

Click “Save” to save these settings.And you can click “Back” to make any modifications. After you click “Save”, it show the following interface.

NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

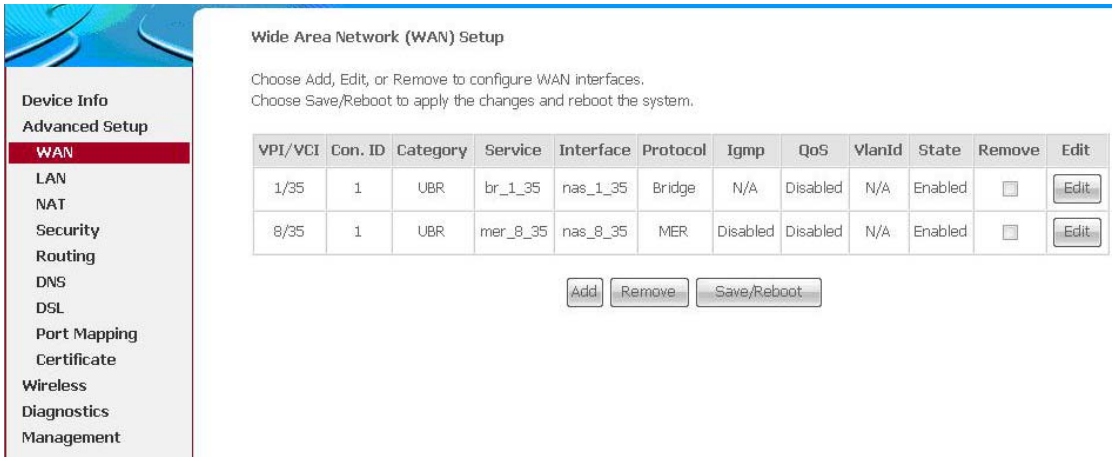
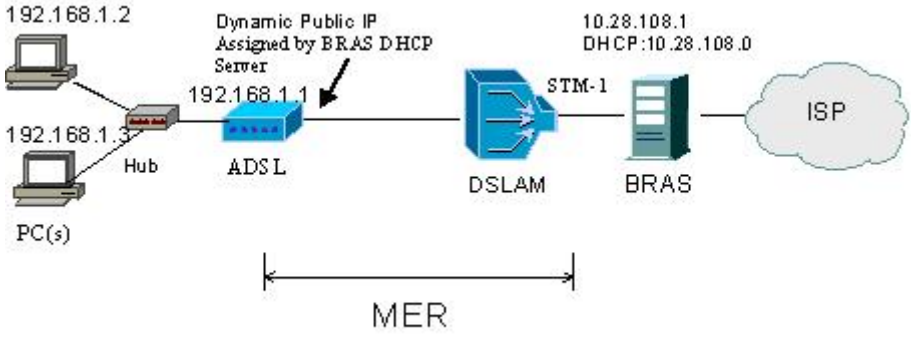


Figure 2.6.6:MER Setup Complete

4.4.1.7 MER PVC Network Application



Descriptions

In this example, the MODEM is connected to the DSLAM through PVC 8/35 and the access mode is the MER+NAT. The downlink interface of BRAS is encapsulated in 1483B, the IP address is 10.28.108.1 and the DHCP Server is enabled, the address pool is 10.28.108.* (2~254), the IP address of the uplink interface is 10.61.92.157; the WAN IP address of the MODEM is automatically obtained through DHCP; the PC attached to the MODEM is assigned with a private IP address (within the same segment as the management IP address 192.168.1.1); the NAT functions of the MODEM is enabled, and the private address of the PC is translated into the public address 10.28.108.* (2~254) dynamically assigned by BRAS for accessing the ISP.

The IP address of the PC can be fixed (as in this example) or assigned through DHCP Server of the MODEM. If it is assigned by the DHCP Server, the DHCP functions of the MODEM must be enabled. The IP address of the DHCP address pool is 192.168.1.* (2~254). The functions are enabled by default and at the same time the PC is configured to obtain IP and DNS addresses dynamically.

Setting

1. Activate your browser and input “192.168.1.1” in the address column to login the MODEM.
2. Click “**Advanced Setup**” -> “**WAN**”, then click “add”.
3. In the “**ATM PVC Configuration”** interface configure VPI/VCI as 8/35 and then click “Next”.
4. In the “**Connection Type**” interface, select “ MAC Encapsulation Routing (MER)” and “LLC/SNAP-BRIDGING” as the encapsulation, and then click “Next”.

5. In the "**WAN IP Settings"** interface, select "Obtain an IP address automatically", "Obtain default gateway automatically" and "Obtain a DNS server address automatically". And then click "Next".

   Note: The WAN IP address, default gateway, and DNS server address can be configured manually.

6. In the "**Network Address Translation Settings**" interface, enable the NAT and firewall. And the other keep the default configuration unchanged . Then click "Next".

7. Check the network configurations and make sure that all settings agree with the data provided by your ISP, and then click "Save".

8. Click "Save/Reboot" to apply the changes and reboot the system.

You can also modify the PVC 8/35. If you need to modify the LAN IP address and DHCP server information, you can do it in "LAN" in "Advanced Setup".
After the configuration is done, the IP address that the MODEM obtains at the WAN-side port nas_8_35. Query "Device Info" → "Route" and the routing table is as follows:

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0
10.28.108.0	0.0.0.0	255.255.255.0	U	0	mer_8_35	nas_8_35
0.0.0.0	10.28.108.1	0.0.0.0	UG	0	mer_8_35	nas_8_35

If "Enable NAT" is disabled during the configuration, you must configure the route on the BRAS; otherwise you cannot access your ISP. In applications, "Enable NAT" must be checked.

4.4.1.8 Add IPoA PVC

Click "Add" to add a certain piece of PVC. The following descriptions are given by an example of adding "PVC 8/35" (IPoA mode).

- Click "Add" following "PVC 8/35".

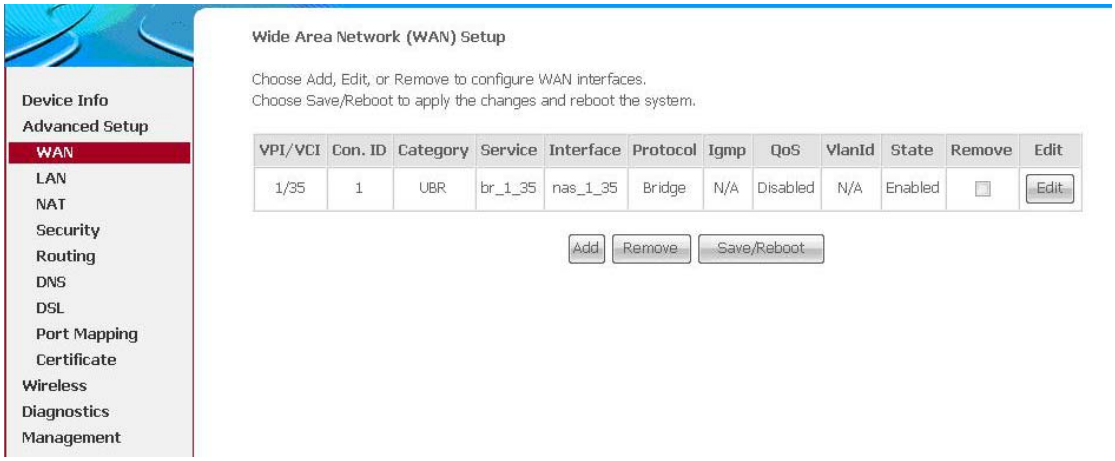


Figure 2.6.7:IPoA Config

- In this interface, you can modify VPI/VCIs, service categories and QoS.

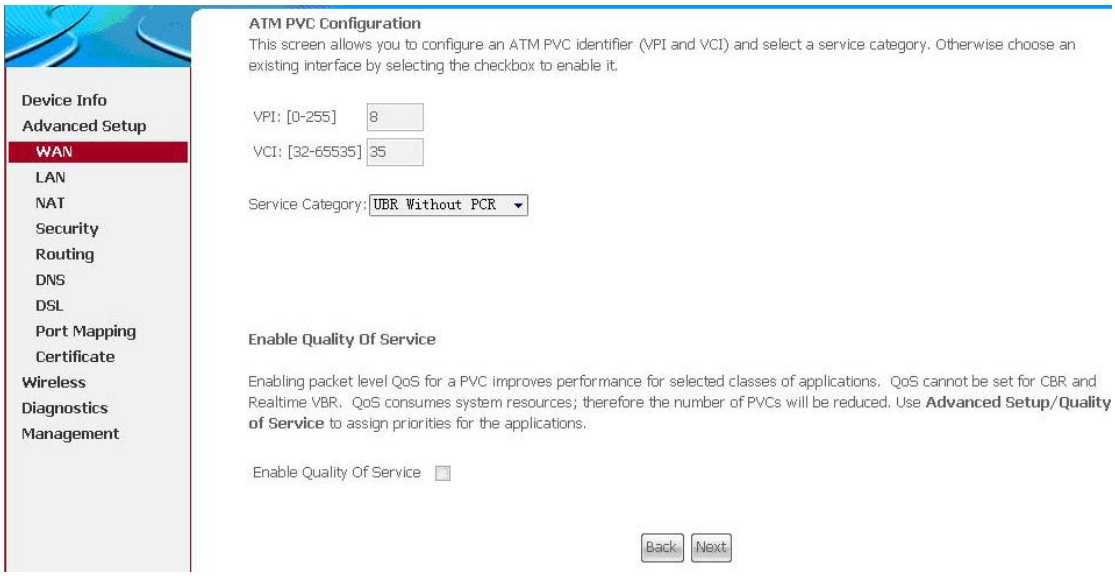

Device Info
Advanced Setup
WAN
LAN
NAT
Security
Routing
DNS
DSL
Port Mapping
Certificate
Wireless
Diagnostics
Management
ATM PVC Configuration
This screen allows you to configure an ATM PVC identifier (VPI and VCI) and select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.
VPI: [0-255] 8
VCI: [32-65535] 35
Service Category: UBR Without PCR
Enable Quality Of Service
Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use Advanced Setup/Quality of Service to assign priorities for the applications.
Enable Quality Of Service
Back
Next

Figure 2.6.8: PVC and it's Qos config page

VPI (Virtual Path Identifier): The virtual path between two points in an ATM network, and its valid value is from 0 to 255.

VCI (Virtual Channel Identifier): The virtual channel between two points in an ATM network, ranging from 32 to 65535 (1 to 31 are reserved for known protocols).

Service Category: UBR Without PCR/UBR With PCR/CBR/Non Realtime VBR/Realtime VBR.

Enable Quality Of Service: enable/disable.

In this example, PVC 8/35 is required to modify, so service category and QoS will remain default values. In actual applications, you can modify them depending on your practices.

After proper modifications, click "Next" to show the following interface.

- In this interface, you can modify Internet Connection Type and Encapsulation Type.

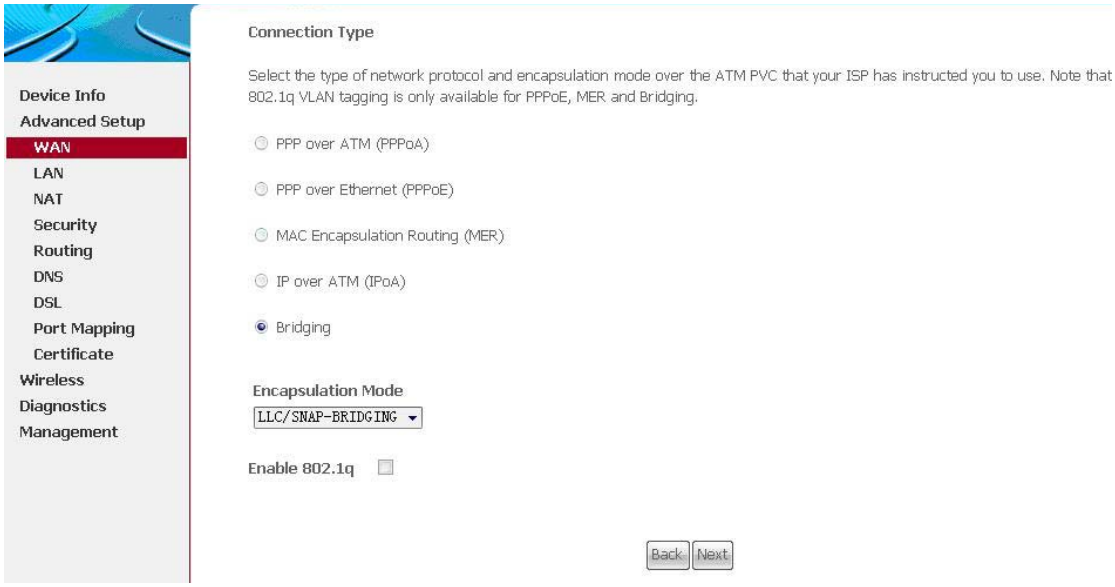


Figure 2.6.9: Internet Connection Type and Encapsulation Type page

Change the connection type of PVC 8/35 to "IP over ATM (IPoA)".

Select "IP over ATM (IPoA)", and "LLC/SNAP-ROUTING" (depending on the uplink equipment, generally "LLC/SNAP-ROUTING") as "Encapsulation Mode".

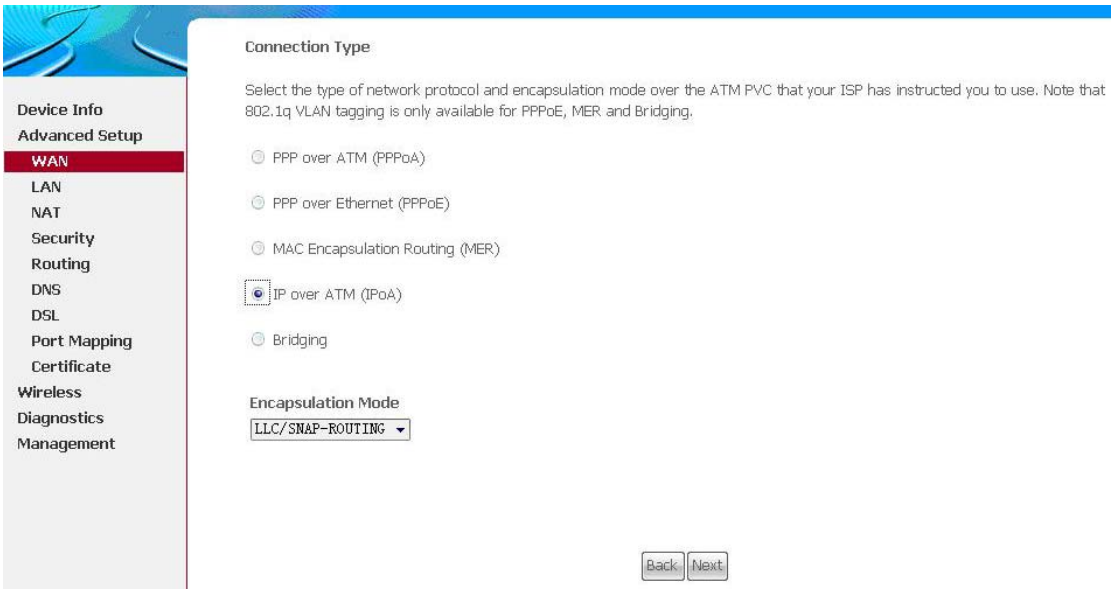


Figure 2.6.10: IP over ATM (IPoA)

Click “Next” to show the following interface.

- In this interface, you can modify the WAN IP, Default Gateway and DNS Server settings.

Figure 2.7.1:IPoA WAN IP Setting

WAN IP Address: Input the IP address of the WAN interface provided by your ISP.
WAN Subnet Mask: Input the subnet mask concerned to the IP address of the WAN interface provided by your ISP.
Obtain Default Gateway automatically: To obtain the IP address of the default gateway assigned by the uplink equipment such as BAS.
Use the following Default Gateway: If you want to input the IP address of the default gateway by yourself, click this entry and then input related data in the fields.
Otherwise to obtain the IP address of the default gateway assigned by the uplink equipment such as BAS.
Use IP Address: Input the gateway of the WAN interface provided by your ISP.
Use WAN Interface: As to BAS equipment, it is the IP address of the downlink interface.
Obtain DNS server address automatically: To obtain the IP address of the DNS server assigned by the uplink equipment such as BAS.
Use the following DNS server addesses: If you want to input the IP address of the DNS server by yourself, click this entry and then input related data in the fields.
Primary DNS server: Input the IP address of the primary DNS server here.
Secondary DNS server: Input the IP address of the secondary DNS server provided by your ISP here.

After correctly modifications, click “Next” to show the following interface.

- In this interface, you can modify the Service name and enable/disable the NAT, Firewal, IGMP Multicast, WAN Service.

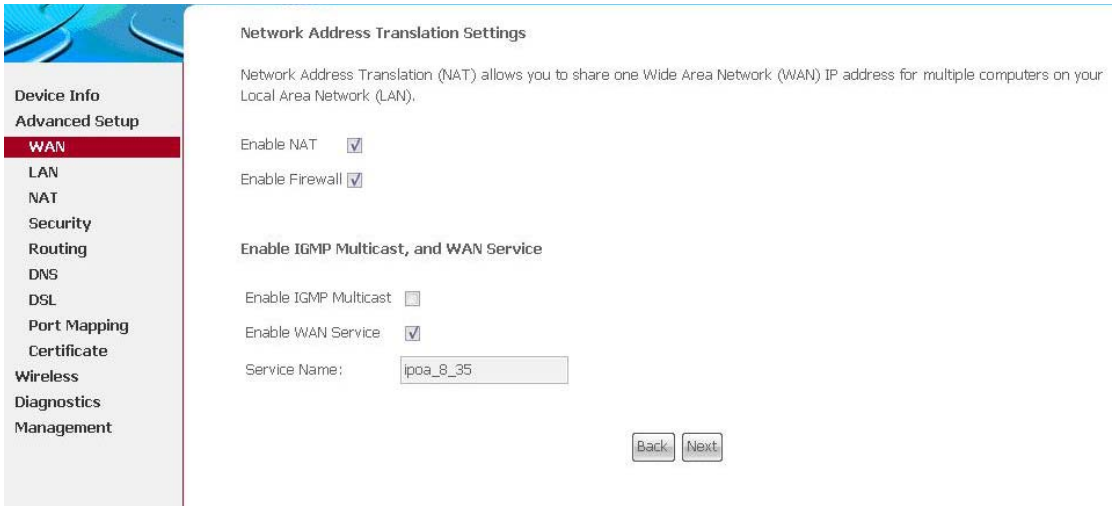


Figure 2.7.2:IPoA IGMP and WAN service page

Enable NAT: Select it to enable the NAT functions of the MODEM. If you are not to enable NAT and intend the user of the MODEM to access the Internet normally, you must add a route on the uplink equipment; otherwise the access to the Internet will fail. Normally, it is required to enable NAT.

Enable Firewall: enable/disable IP filtering.

IGMP Multicast: IGMP proxy. For example, if you need IPoA mode support IPTV, please enable it.

WAN Service: Please enable it, unless you don’t need to active the PVC.

Click “Next” to show the following interface.

- In this interface, it show the all configuration.

Figure 2.7.3:IPoA Setup Summary

Click “Save” to save these settings.And you can click “Back” to make any modifications. After you click “Save”, it show the following interface.

NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

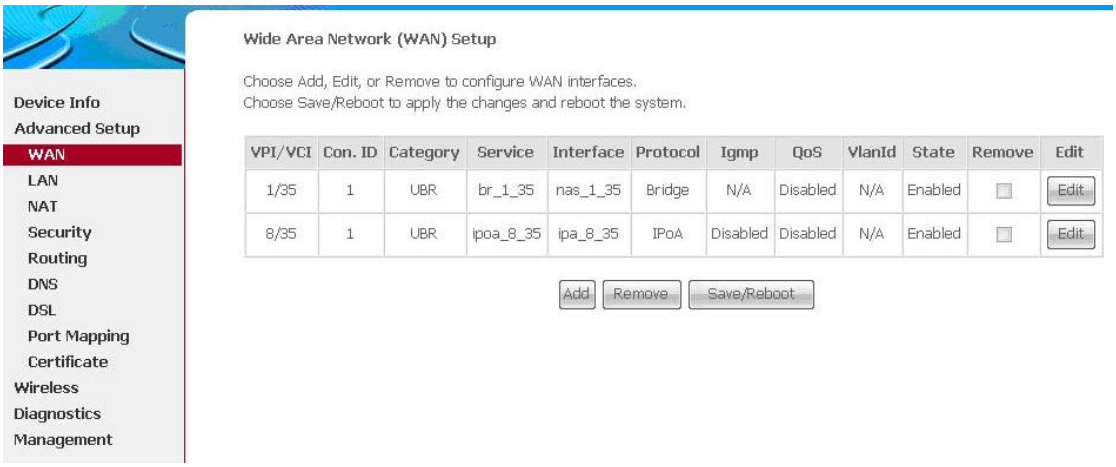
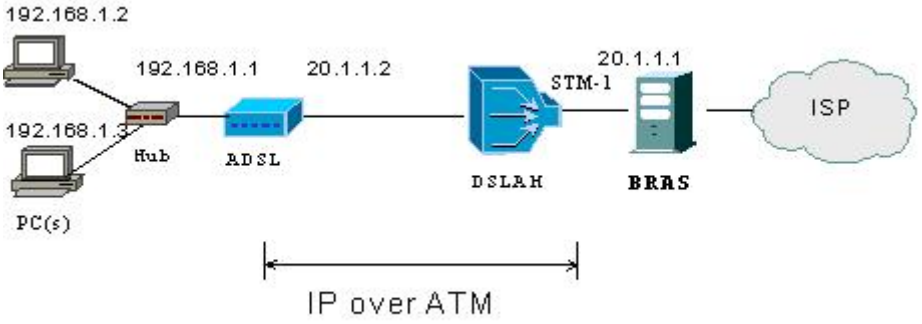


Figure 2.7.4:IPoA Setup Complete

4.4.1.9 IPoA PVC network application



Descriptions

In this example, the MODEM is connected to the DSLAM through PVC 8/35 and the access mode is the IPOA+NAT. The downlink interface of BRAS is encapsulated in 1483R, the IP address is 20.1.1.1, the IP address of the uplink interface is 10.61.92.157; the WAN IP address of the MODEM is assigned as 20.1.1.2; the PC attached to the MODEM is assigned with a private IP address (within the same segment as the management IP address 192.168.1.1); the NAT functions of the MODEM is enabled, and the private address of the PC is translated into the public address 139.1.1.* (2~254) dynamically assigned by BRAS for accessing the ISP.

The IP address of the PC can be fixed (as in this example) or assigned through DHCP Server of the MODEM. If it is assigned by DHCP Server, the DHCP functions of the MODEM must be enabled. The IP address of the DHCP address pool is 192.168.1.* (2~254). The functions are enabled by default and at the same time the PC is configured to obtain IP and DNS addresses dynamically.

Setting

1. Activate your browser and input “192.168.1.1” in the address column to login the MODEM.
2. Click “**Advanced Setup**” -> “**WAN**”, then click “add”.
3. In the “**ATM PVC Configuration”** interface configure VPI/VCI as 8/35 and then click “Next”.
4. In the “**Connection Type**” interface, select “ IP over ATM (IPoA)” and “LLC/SNAP-ROUTING” as the encapsulation, and then click “Next”.
5. In the “**WAN Setting**s” interface, input the IP address, subnet mask, and DNS server address provided by your ISP. Don’t select “Use the following default gateway”. And then click “Next”.

   WAN IP Address: 20.1.1.2
   WAN Subnet Mask: 255.255.255.0
   Primary DNS server: 168.95.1.1

Secondary DNS server: 168.95.192.1

6. In the "**Network Address Translation Settings**" interface, enable the NAT and firewall. And the other keep the default configuration unchanged . Then click "Next".
7. Check the network configurations and make sure that all settings agree with the data provided by your ISP, and then click "Save".
8. Click "Save/Reboot" to apply the changes and reboot the system.

You can also modify the PVC 8/35. If you need to modify the LAN IP address and DHCP server information, you can do it in "LAN" in "Advance".
After the configuration is done, the MODEM WAN-side interface is ipa_8_35.

If "Enable NAT" is disabled during the configuration, you must configure the route on the BRAS; otherwise you cannot access your ISP. In applications, "Enable NAT" must be checked.

4.4.1.10 Add Bridge PVC

Click "Add" to add a certain piece of PVC. The following descriptions are given by an example of adding "PVC 8/35" (IPoA mode).

- Click "Add" following "PVC 8/35".

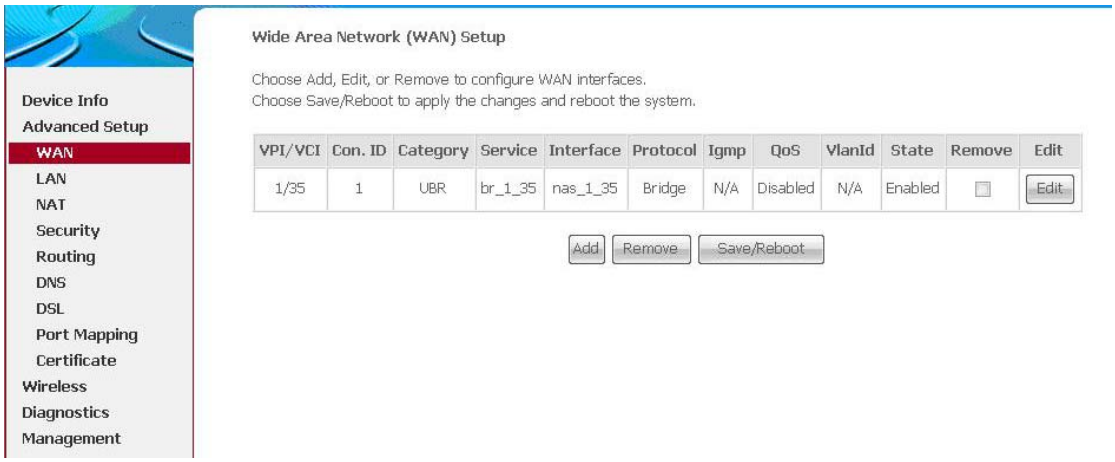


Figure 2.7.5:Bridge Config

- In this interface, you can modify VPI/VCIs, service categories and QoS.

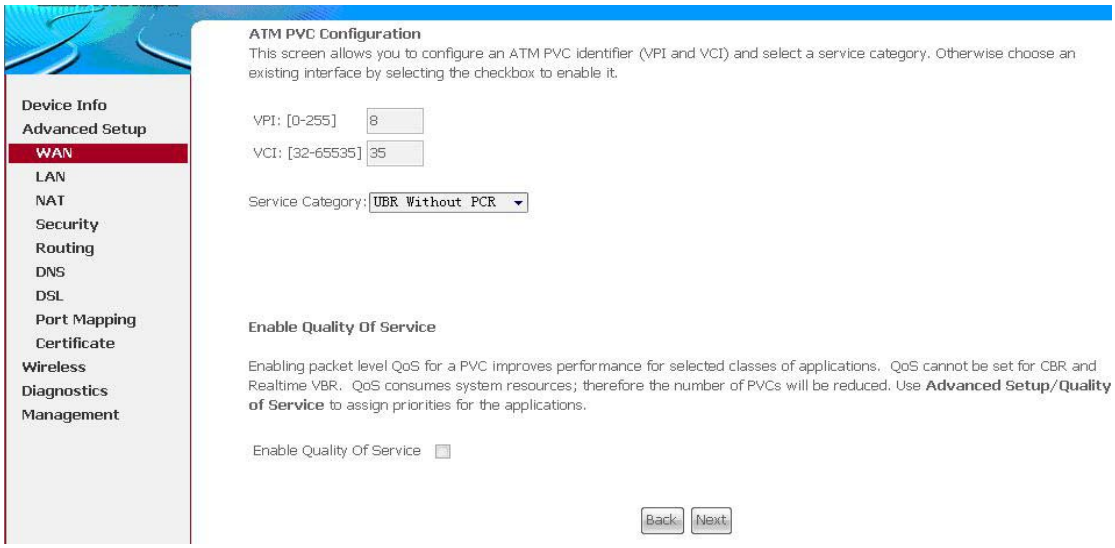

ATM PVC Configuration
This screen allows you to configure an ATM PVC identifier (VPI and VCI) and select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Routing
DNS
DSL
Port Mapping
Certificate
Wireless
Diagnostics
Management
VPI: [0-255] 8
VCI: [32-65535] 35
Service Category: UBR Without PCR
Enable Quality Of Service
Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use Advanced Setup/Quality of Service to assign priorities for the applications.
Enable Quality Of Service
Back Next

Figure 2.7.6: Internet Connection Type and Encapsulation Type page

VPI (Virtual Path Identifier): The virtual path between two points in an ATM network, and its valid

value is from 0 to 255.

VCI (Virtual Channel Identifier): The virtual channel between two points in an ATM network, ranging from 32 to 65535 (1 to 31 are reserved for known protocols).

Service Category: UBR Without PCR/UBR With PCR/CBR/Non Realtime VBR/Realtime VBR.

Enable Quality Of Service: enable/disable.

In this example, PVC 8/35 is required to modify, so service category and QoS will remain default values. In actual applications, you can modify them depending on your practices.

After proper modifications, click “Next” to show the following interface.

- In this interface, you can modify Internet Connection Type and Encapsulation Type.

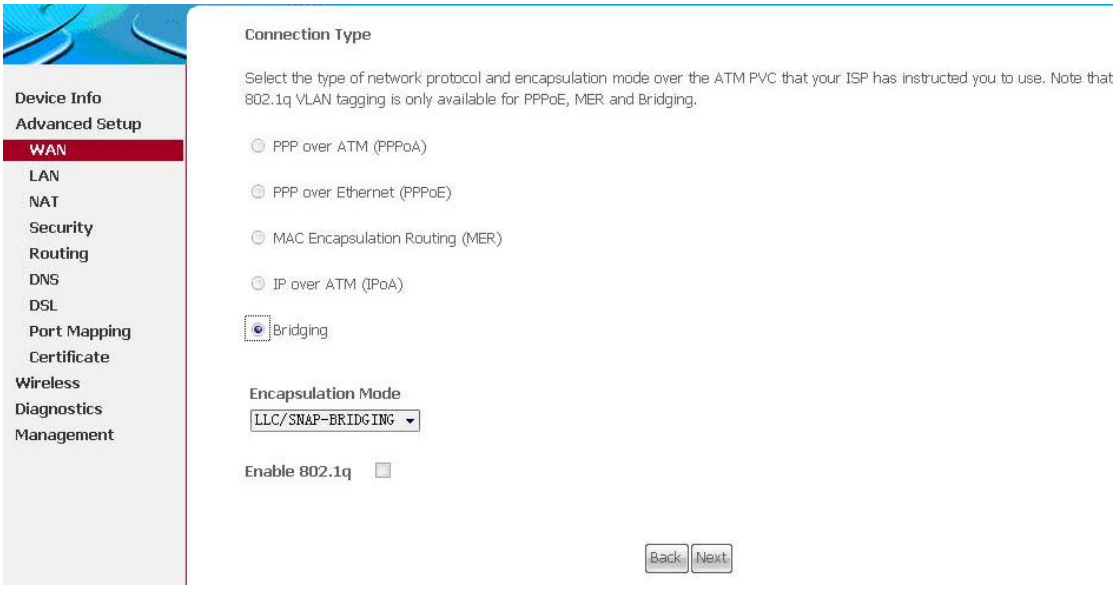


Figure 2.7.7:Bridge

Enable 802.1q: If enable it, input the 802.1q VLAN tag value. Note that 802.1q VLAN tagging is only available for PPPoE, MER and Bridge.

Click “Next” to show the following interface.

- In this interface, you can modify the Service name.

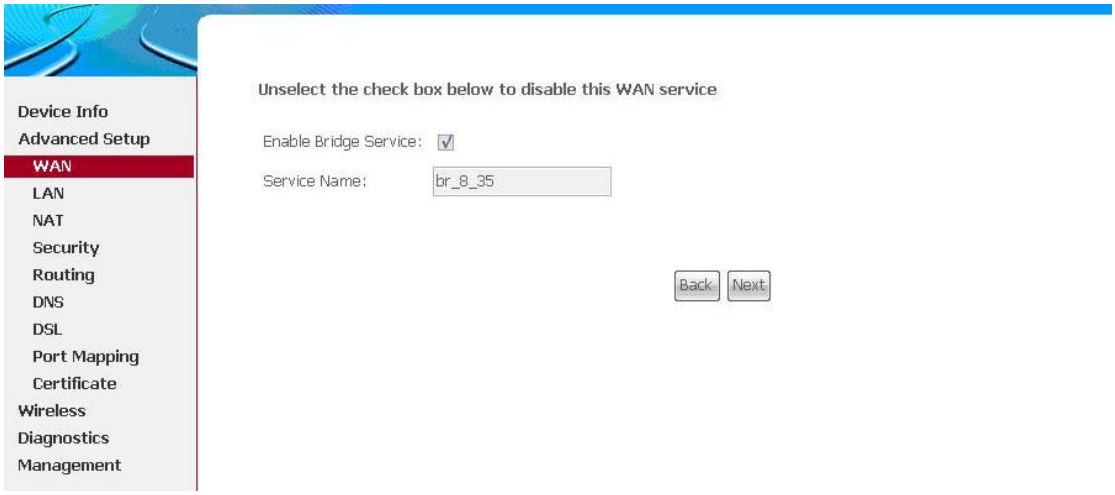


Figure 2.7.8:Bridge service page

WAN Service: Please enable it, unless you don’t need to active the PVC.

Click “Next” to show the following interface.

- In this interface, it show the all configuration.

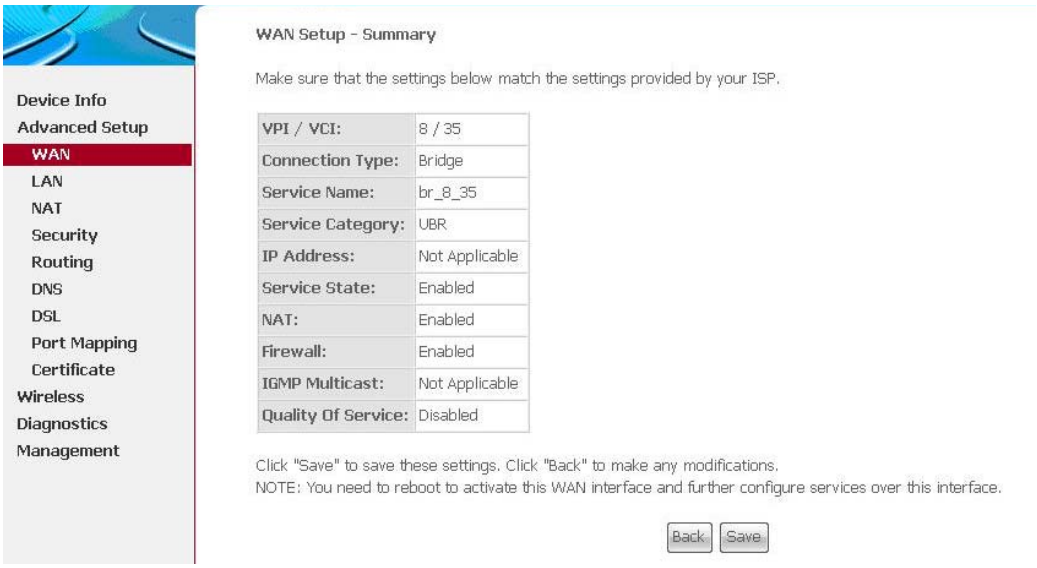


Figure 2.7.9:Bridge Setup Summary

Click “Save” to save these settings.And you can click “Back” to make any modifications. After you click “Save”, it show the following interface.

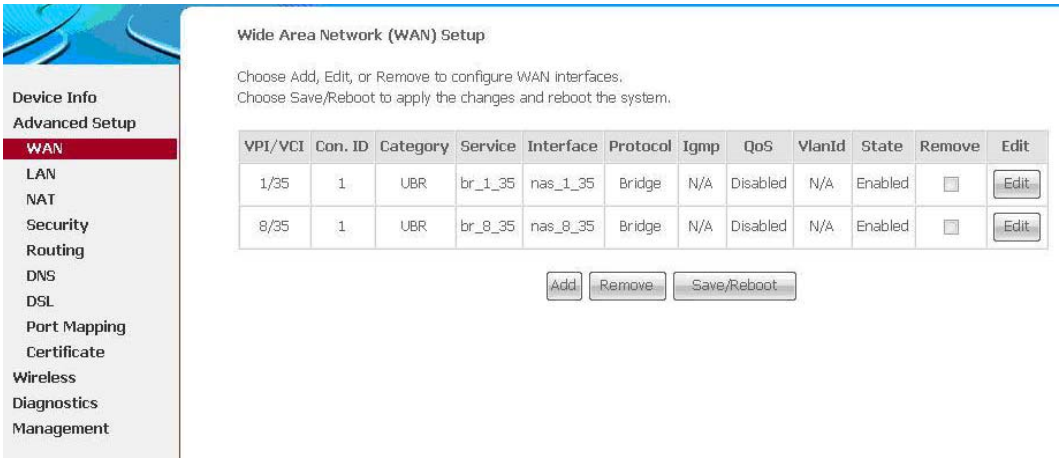
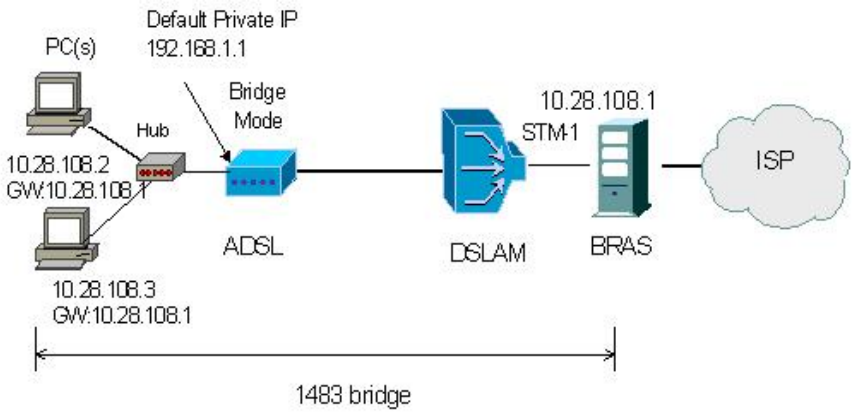


Figure 2.7.10:Bridge Setup Complete

NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

4.4.1.11 Bridge PVC Network Application



Descriptions
In this example, the MODEM is connected to the DSLAM through PVC 8/35 and the access mode is pure Bridging. The uplink interface of BRAS is encapsulated as 1483B, the IP address is 10.28.108.1, the IP address of the uplink interface is 10.61.92.157. The PC attached to the MODEM is assigned a public IP address and the gateway is 10.28.108.1.
Setting

1. Activate your browser and input "192.168.1.1" in the address column to login the MODEM.
2. Click "**Advanced Setup**" -> "**WAN**", then click "add".
3. In the "**ATM PVC Configuration"** interface configure VPI/VCI as 8/35 and then click "Next".
4. In the "**Connection Type**" interface, select "Bridging" and "LLC/SNAP-BRIDGING" as the encapsulation, and then click "Next".
5. In the "**Unselect the check box below to disable this WAN service**" interface, keep the default configuration unchanged and then click "Next".
6. Check the network configurations and make sure that all settings agree with the data provided by your ISP, and then click "Save".
7. Click "Save/Reboot" to apply the changes and reboot the system.

You can also modify the PVC 8/35. If you need to modify the LAN IP address, you can do it in "LAN" of "Advance".
Note: In the pure Bridging mode, there is no interface at the WAN side of the MODEM.

4.4.1.12 Remove Pvc

4.4.2 LAN configuration

You can use the LAN configuration to define an IP address for the DSL Router and configure the DHCP server

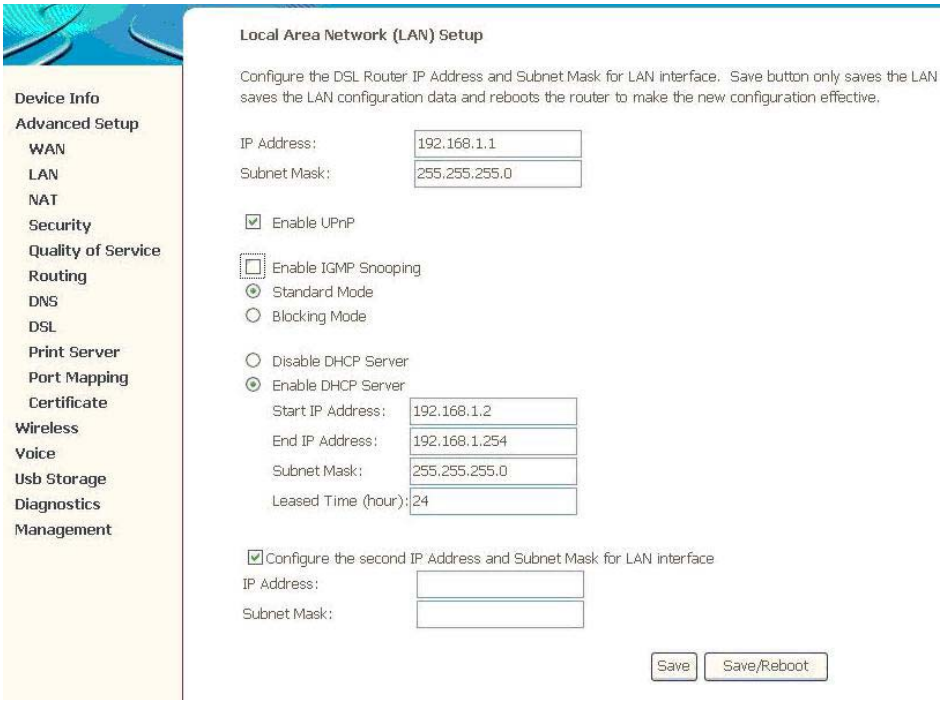


Figure 2.8.1: LAN configuration setup

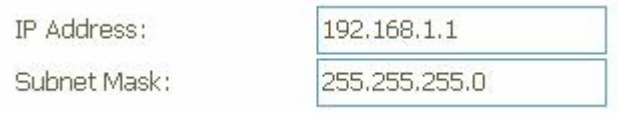
4.4.2.1 Defining the private IP address for the DSL Router

On this screen you can change the device's IP address. The preset IP address is 192.168.1.1. This is the Private IP address of the DSL Router. This is the address under which the device can be reached in the

local network. It can be freely assigned from the block of available addresses. The IP address under which the DSL ROUTE WLAN dsl can be reached from outside is assigned by the Internet service provider.

- If you want to assign a different IP address to the DSL Router, enter it in the fields next to IP address.
- Adjust the Subnet mask if necessary.

We recommend that you use an address from a block that is reserved for private use.
This address block is 192.168.1.1-192.168.255.254



Note:
New settings can only be made after the DSL Router has been rebooted. If necessary, reconfigure the IP address on your PC (including one that is statically assigned) so that it matches the new configuration.

4.4.2.2 Enable UPNP (Universal Plug and Play)

PCs with UPnP (Universal Plug & Play) can offer their own network services and automatically use services offered in the network.

Note:
The PC must have WindowsME or WindowsXP as its operating system. Check whether the UPnP function has been installed in the PC's operating system. It may be necessary to retrospectively install the UPnP components, even on systems with WindowsXP or WindowsME. Please consult your PC's user guide.

As soon as you have installed UPnP in the operating system of a PC and activated it on the router, applications on this PC (e.g. Microsoft Messenger) can communicate via the Internet without you needing to expressly authorise it. In this case, the router automatically implements port forwarding, thereby facilitating communication via the Internet.The task bar on the PC on which UPnP is installed contains an icon for the DSL Router. In systems with WindowsXP, the icon is also shown undernetwork connections. Click this icon to open the user interface of the DSL Router.

Note:
When the UPnP function is active, system applications can assign and use Ports on a PC. This poses a security risk.

4.4.2.3 Enable IGMP Snooping

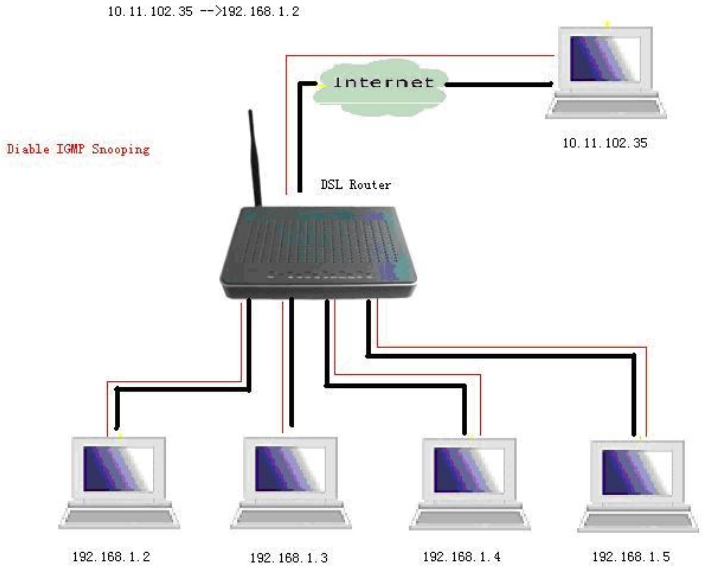


Figure 2.8.2: Diable IGMP Snooping

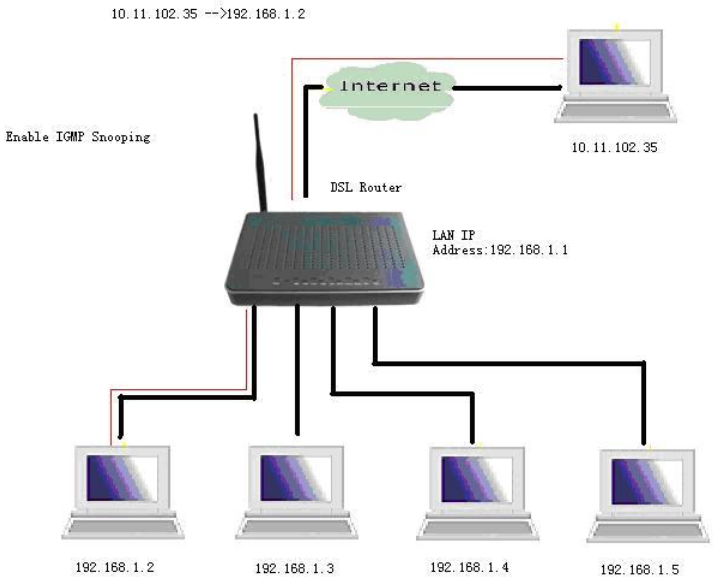


Figure 2.8.3: Enable IGMP Snooping

Internet Group Management Protocol

IGMP is an Internet Protocol that enables an Internet computer to inform neighbouring routers that it is a member of a multicast group. With multicasting, a computer can send content on the Internet to several other computers that have registered an interest in the first computer's content. Multicasting can, for example, be used for multimedia programs for media streaming to recipients that have set up multicast group membership.

Note:

If IGMP Snooping function is actice ,DSL Router capability will improve

4.4.2.4 Configuring the DHCP server

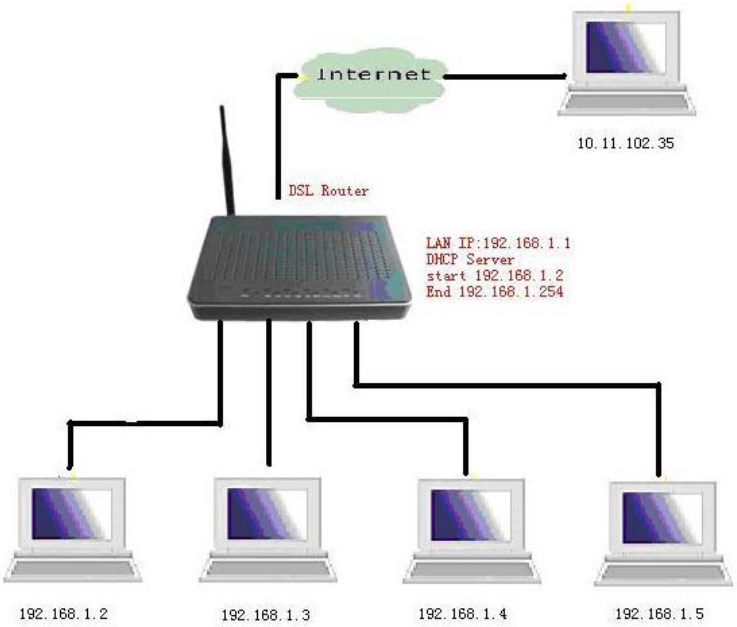


Figure 2.8.4:DHCP Server

The DSL ROUTE has a DHCP server for which the factory setting is active. Consequently, the IP

addresses of the PCs are automatically assigned by the DSL Router.

Note:

- If the DHCP server for the DSL Router is activated, you can configure the network setting on the PC so that the option Obtain an IP address automat-ically is set up. Further information about this can be found in the section entitled
- If you deactivate the DHCP server, you will have to assign a static IP address for the PCs that use the network settings

- To activate the DHCP server, select On.
- If the DHCP server is active, you can define a Lease time. The Lease time determines the period for which the PCs retain the IP addresses assigned to them without chang-ing them.

Note:

If you select Never expires, the IP addresses are never changed. Activate this option if you want to make NAT or firewall settings using the IP addresses of the PCs; otherwise you have to assign static IP addresses to these PCs.

- Define the range of IP addresses the DSL Router WLAN dsl should use to auto-matically assign IP addresses to the PCs. Define the First issued IP address and the Last issued IP address.

4.4.2.5 Configure the second IP Address and Subnet Mask for lan interface

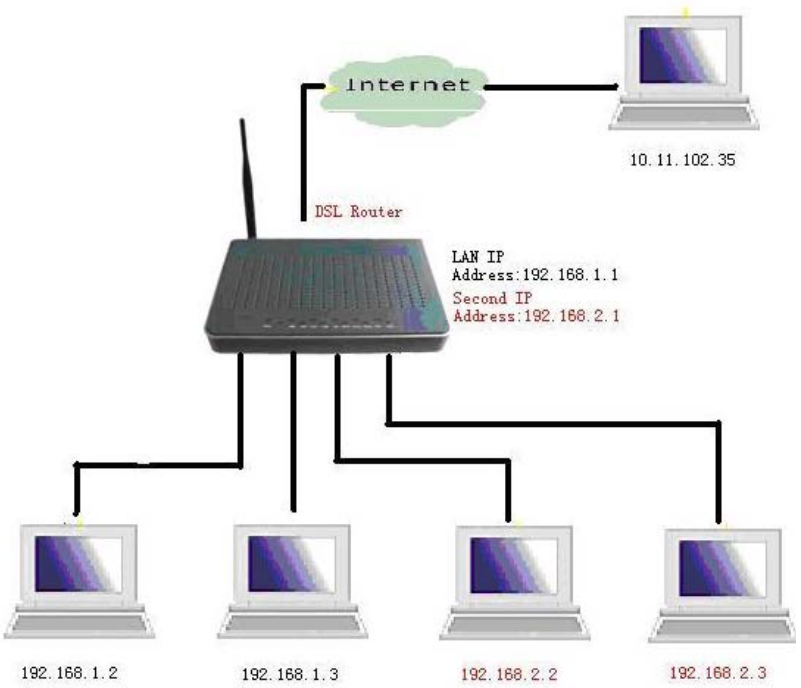


Figure 2.8.5:Second IP Address

This point explain in “Defining the private IP address for the DSL Router”

4.4.3 NAT-- Network Address Translation

4.4.3.1 Overview

Setting up the NAT function

- The DSL Router comes equipped with the NAT (Network Address Translation) function. With address mapping, several users in the local network can access the Internet via one or more public IP addresses. All the local IP addresses are assigned to the router's public IP address by default.

- One of the characteristics of NAT is that data from the Internet is not allowed into the local network unless it has been explicitly requested by one of the PCs in the network. Most Internet applications can run behind the NAT firewall without any problems. For example, if you request Internet pages or send and receive e-mails, the request for data from the Internet comes from a PC in the local network, and so the router allows the data through. The router opens precisely one port for the application. A port in this context is an internal PC address, via which the data is exchanged between the Internet and a client on a PC in the local network. Communicating via a port is subject to the rules of a particular protocol (TCP or UDP).

- If an external application tries to send a call to a PC in the local network, the router will block it. There is no open port via which the data could enter the local network.Some applications, such as games on the Internet, require several links, i.e. several ports so that the players can communicate with each other. In addition, these applications must also be permitted to send requests from other users on the Internet to users in the local network. These applications cannot be run if Network Address Translation (NAT) has been activated.

- Using port forwarding (the forwarding of requests to particular ports) the router is forced to send requests from the Internet for a certain service, e.g. a game, to the appropriate port(s) on the PC on which the game is running. Port triggering is a special variant of port forwarding. Unlike port forwarding, the DSL Router forwards the data from the port block to the PC which has previously sent data to the Internet via a certain port (trigger port). This means that approval for the data transfer is not tied to one specific PC in the network, but rather to the port numbers of the required Internet service.Where configuration is concerned, this means: You have to define a so-called trigger port for the application and also the protocol (TCP or UDP) that this port uses. You then assign the public ports that are to be opened for the application to this trigger port. u The router checks all outgoing data for the port number and protocol. If it identifies a match of port and protocol for a defined trigger port, then it will open the assigned public ports and notes the IP address of the PC that sent the data. If data comes back from the Internet via one of these public ports, the router allows it through and directs it to the appropriate PC. A trigger event always comes from a PC within the local network. If a trigger port is addressed from outside, the router simply ignores it.

Note:

- An application that is configured for port triggering can only be run by one user in the local network at a time.
- As long as the public ports are open, they can be used by unauthorised persons to gain access to a PC in the local network.

When the DSL Router is supplied, the NAT function (Network Address Translation) is activated, i.e. all IP addresses of PCs in the local network are converted to the router's public IP address when accessing the Internet. You can use the NAT settings to configure the DSL Router to carry out the following tasks:

Note:

For the functions described below, the IP addresses of the PCs must remain unchanged. If the IP addresses of the PCs are assigned via the DHCP server of the DSL Router, you must select Never expires (see page79) as the settings in the Local Network menu entry for the Lease time or assign static IP addresses for the PCs.

You can activate or deactivate the NAT function (by default the NAT function is activated).

4.4.3.2 NAT -- Virtual Servers Setup

In its default state, DSL router blocks all external users from connecting to or communicating with your net-work. Therefore the system is safe from hackers who may try to intrude on the network and damage it. However, you may want to expose your network to the Internet in certain limited and controlled ways in order to enable some applications to work from the LAN (game, voice and chat applications, for example) and to enable Internet-access to servers in the home network. The Port Forwarding feature supports both of these functionalities. If you are familiar with networking terminology and concepts, you may have encountered this topic referred to as “Local Servers” The Port Forwarding screen lets you define the applications that require special handling by DSL router .All you have to do is select the application protocol and the local IP address of the computer that will be using or providing the service. If required, you may add new protocols in addition to the most common ones provided by DSL router. For example, if you wanted to use a File Transfer Protocol (FTP) application on one of your PCs, you would simply select FTP from the list and enter the local IP address or host name of the designated computer. All FTP-related data arriving at DSL router from the Internet will henceforth be forwarded to the specific computer.Similarly, you can grant Internet users access to servers inside your home network, by identifying each service and the PC that will provide it. This is useful, for example, if you want to host a Web server inside your home network. When an Internet user points his/her browser to DSL router external IP address, the gateway will forward the incoming HTTP request to your Web server.With one external IP address (DSL router main IP address), different applications can be assigned to your LAN computers, however each type of application is limited to use one computer. For example, you can de net hat FTP will use address X to reach computer A and Telnet will also use address X to reach computer A, but attempting to define FTP to use address X to reach both computer A and B will fail. DSL router therefore provides the ability to add additional public IP addresses to port forwarding rules, which you must obtain from your ISP, and enter into the NT IP Addresses Pool (see section 7.3.7). You will then be able to define FTP to use address X to reach computer A and address Y to reach computer B. Additionally, port forwarding enables you to redirect traffic to a different port instead of the one to which it was designated. Lets say, that you have a Web server running on your PC on port 8080 and you want to grant access to this server to any one who accesses DSL router via HTTP To accomplish this, do the following:

- De fine a port forwarding rule for the HTTP service, with the PC IP or host name.
- Specify 8080 in the Forward to Port’ field.

All incoming HTTP traffic will now be forwarded to the PC running the Web server on port 8080 When setting a port forwarding service, you must ensure that the port is not already in use by another application, which may stop functioning. A common example is when using SIP signaling in Voice over IP the port used by the gateway VoIP application (5060) is the same port on which port forwarding is set for LAN SIP agents.

> Note:
> Some applications, such as FTP, TFTP, PPTP and H323, require the support of special specific Application Level Gateway(ALG) modules in order to work inside the home network. Data packets associated with these applications contain information that allows them to be routed correctly. An ALG is needed to handle these packets and ensure that they reach their intended destinations. DSL router is equipped with a robust list of ALG modules in order to enable maximum functionality in the home network The ALG is automatically assigned based on the destination port

Virtual Servers is configured for this purpose.

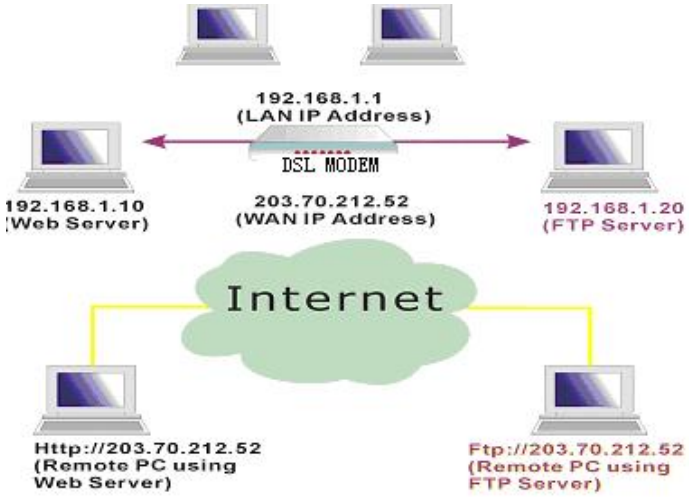


Figure: 2.8.6: Virtual Servers

Add Port Forwarding

- To set up Virtual Servers for a service, select Virtual Servers from the Advanced Setup –-NAT-- Virtual Servers Setup--add

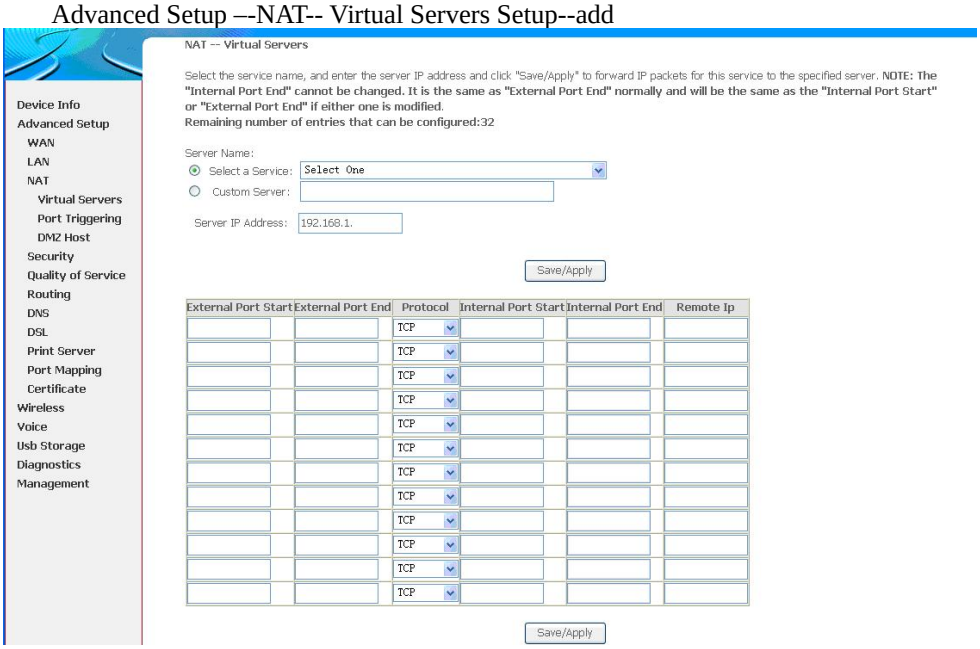


Figure: 2.8.6.1: Add virtual Servers

- Select a service ,or custom your server
- Set Server IP address
- Enter the Set Server IP address of the computer that will provide the service(the server in the Local Host field. Note that unless an additional external IP address has been added, only one LAN computer can be assigned to provide a specific service or application.
- Set External port start external port end
- Select protocol
- Set Internal port start and internal port end
- Entry Remote ip
- Click OK to apply the settings

If the application you require is not in the list, you must manually enter the relevant data on the screen: Select the protocol for the service you are providing from the Protocol list.Under Public port, enter the port number of the service you are providing. In the Local port field, enter the internal port number to which service requests are to be forwarded. In the Local IP address field, enter the IP address of the PC that provides the service.

Example: the Web server has been configured to react to requests on port 8080. However, the requests

from websites enter the Web server via port 80 (standard value). If you add the PC to the forwarding table and define port 80 as the public port and port 8080 as an internal port, all requests from the Internet are diverted to the service with the port number 80 on the Web server of the PC you have defined with port 8080.

> Note:
> You can use a single port number, several port numbers separated by commas, port blocks consisting of two port numbers separated by a dash, or any combination of these, for example 80, 90-140, 180.

Del Port Forwarding

- Click remove box
- Click remove to apply the settings

4.4.3.3 Port Triggering

If you configure port triggering for a certain application, you need to determine a so-called trigger port and the protocol (TCP or UDP) that this port uses. You then assign the public ports that are to be opened for the application to this trigger port. You can select known Internet services or assign ports or port blocks manually.

Add port Triggering

To set up port triggering for a service, select Port Triggering from the Advanced Settings →net→ port Triggering→add

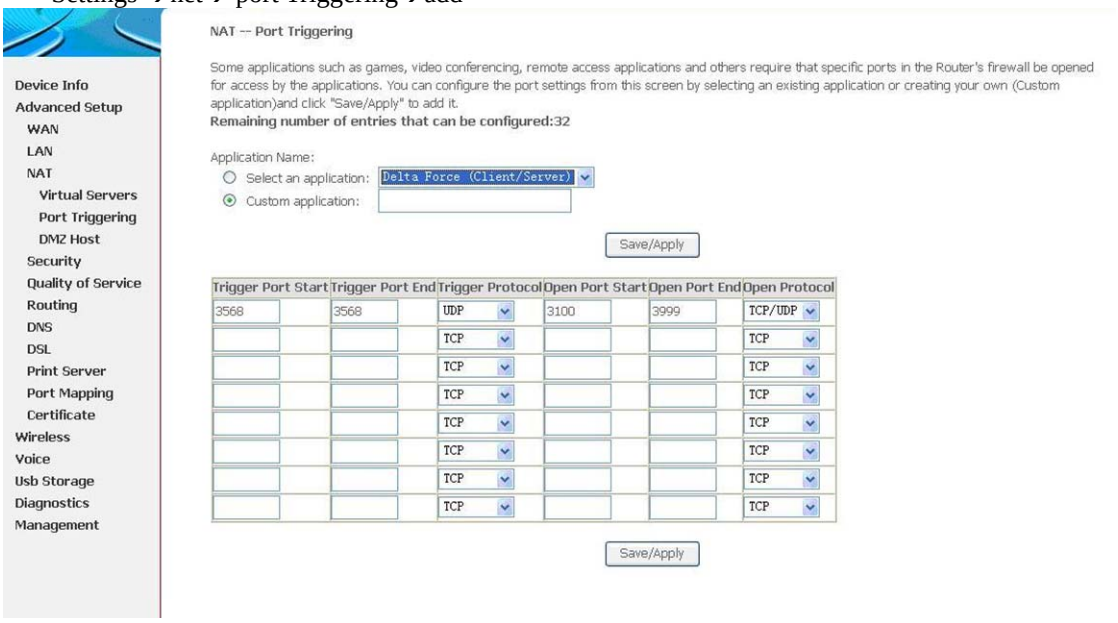


Figure2.8.6.2: Port Triggering

- Select the required application from the applications list.

If the application you require is not in the list, you must enter the relevant data on the screen custom application

- Trigger port start and Trigger port end: Enter the port that is to be monitored for outgoing data traffic.
- trigger protocol: Select the protocol that is to be monitored for outgoing data traffic.
- Open Protocol: Select the protocol that is to be allowed for incoming data traffic
- Open port start and Open port end: Enter the port that is to be opened for incoming traffic.

> Note:
> You can use a single port number, several port numbers separated by commas, port blocks consisting of two port numbers separated by a dash, or any combina-tion of these, for example 80, 90-140, 180.

- Apply the settings by clicking “save/apply”

Remove port Triggering

Check remove box

Apply setting by click Save/Apply

4.4.3.4 DMZ Host

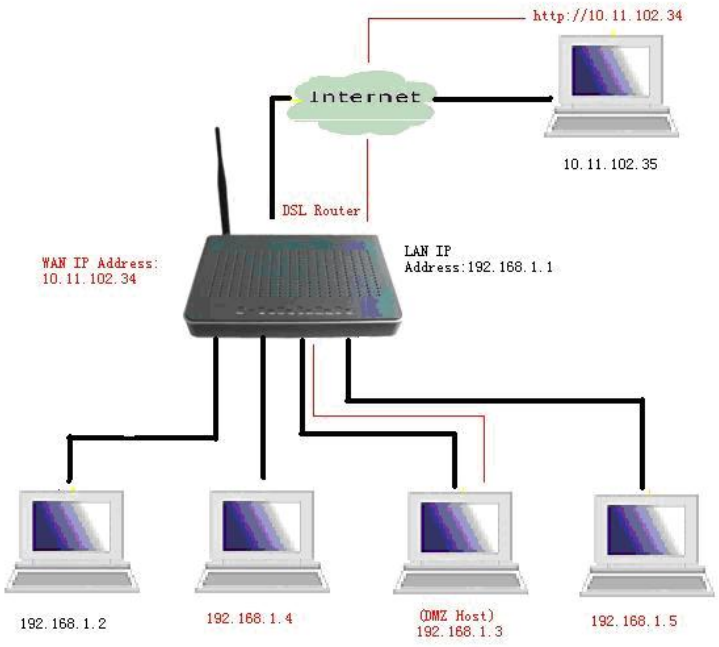


Figure2.8.6.3:DMZ Host

The DMZ (Demilitarized) Host featureallows one local computer to be exposed to the Internet. You wish to use a special-purpose Internet service, such as an on-line game or video-conferencing Program, that is not present in the Port Forwarding list and for which no port range information is available. You are not concerned with security and wish to expose one computer to all services without restriction.

note: A DMZ host is not protected by the rewall and may be vulnerable to attack. Designating a DMZ host may also put other computer sin the home net work at risk. When designnating a DMZ host, you must consider the security implications and protect it if necessary.

You can set up a client in your local network to be a so-called "DMZ host". Your device will then forward all incoming data traffic from the Internet to this client. You can then, for example, operate your own Web server on one of the clients in your local network and make it accessible to Internet users. As the exposed host, the local client is directly visible to the Internet and therefore particularly vulnerable to attacks (e.g. hacker attacks). Only activate this function if it is absolutely necessary (e.g. to operate a Web server) and other functions (e.g. port forwarding) are not adequate. In this case you should take appropriate measures for the clients concerned.

Note:
Only one PC per public IP address can be set up as an Exposed Host

Add an DMZ host

- To set up a PC as an DMZ host, select DMZ Host from the Advanced Setup→NAT→ DMZ host

Figure2.8.6.4 DMZ Host Config

- Enter the Local IP address of the PC that is to be enabled as an Exposed Host.
- Apply the settings by clicking “Save/Apply”.

Remove DMZ host

Clear the DMZ Host Address
Apply setting by click Save/Apply

4.4.4 Security

Security is a important function of DSL, it protects the resources of a private network from users from other networks. Also the item prevent unauthorized internet users form accessing private networks connected to the internet. All messages entering or leaving the intranet (i.e., the local network to which you are connected)must pass through the security examines , which examines each message and blocks those that do not meet the specified security criteria.
There are three basic types of security techniques:

- IP packet filtering: The system examines each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure .
- Ciruit-level gatway implementation: This process applies security mechanisms when a TCP or UDP connection is established . Once the connect has been made, packets can flow between the hosts without further checking.
- MAC frame filtering: The system examines each frame entering or leaving the network form layer 2 . And accord to user-defined rules accepts and rejects frame .

A security management program can be configured one of two basic ways:

- A default-deny policy.
- A defaulte-allow policy.

A default-deny approach to security is by far the more secure, but due to the difficulty inconfiguring and managing a network in that fashion, many networks instead use the default-allow approach. Let's assume for the moment that your security management program utilizes a default-deny policy, and you only have certain services enabled that you want people to be able to use from the Internet.
NOTE: The security is like a firewall.

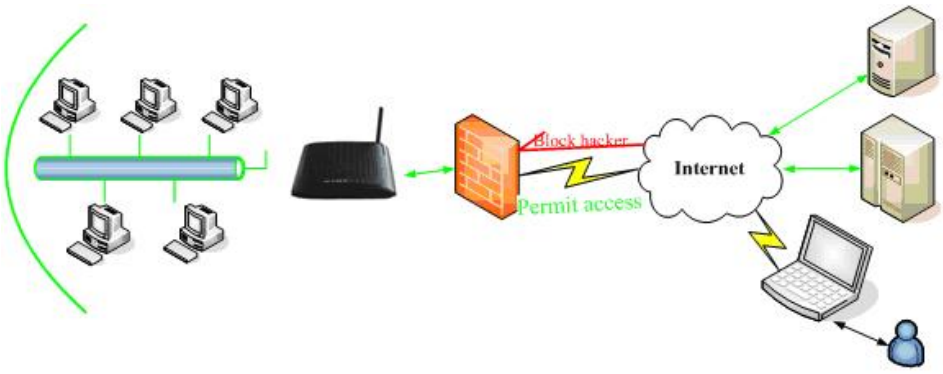


Figure2.8.6.5：the Security application

Click “Security” -->” IP Filtering” to show the following interface. By default, the firewall is enabled. The firewall is used to block document transmissions between the Internet and your PC. It serves as a safety guard and only permits authorized documents to be sent into the LAN.
Note: If the modem configured bridge mode only, the IP Filtering will disabled and the IP filtering interface will disappear.
And if the modem configured no Bridge mode PVC, the MAC Filtering will disabled and the MAC Filtering interface will disappear.

Figure2.8.6.6:Outgoing IP Filtering Setup overview

4.4.4.1 Outgoing IP Filtering Setup

When Outgoing IP Filtering rules setup being enable on the MODEM, the various security functions for the local network will enable at the same time .You can protect the network against hacker attacks and block individual PC’s access to selected services or internet sites.
Click “Security”-->” IP Filtering”-->” Outgoing” to show the following interface.
By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be BLOCKED by setting up filters.

Figure2.8.6.7: Outgoing IP Filtering Config

Click “Add” to enter the related interface defining the IP filtering rule as follows.
The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.

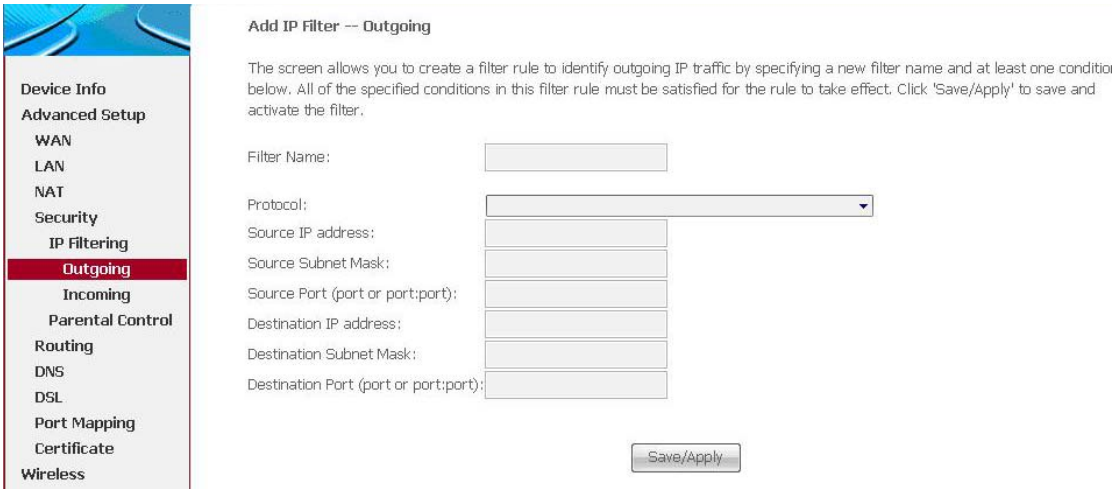


Figure2.8.6.8: Outgoing IP Filtering Add Setup

Filter Name: Enter the name of outgoing filter rule
Protocol: select one among TCP/UDP TCP UDP or ICMP protocols
Source IP address Enter a ip address.when you have set ip address ,the outgoing packet (protocol selected packet) will block.
Source subnet mask
Source port : UPD/TCP source port or a range of ports
Destination IP address: destination ip (default no set)
Destination subnet mask:
Destination port : UPD/TCP destination port or a range of ports

There is a examples to introduce how to configure the outgoing IP Filtering.
The topology is as follows:

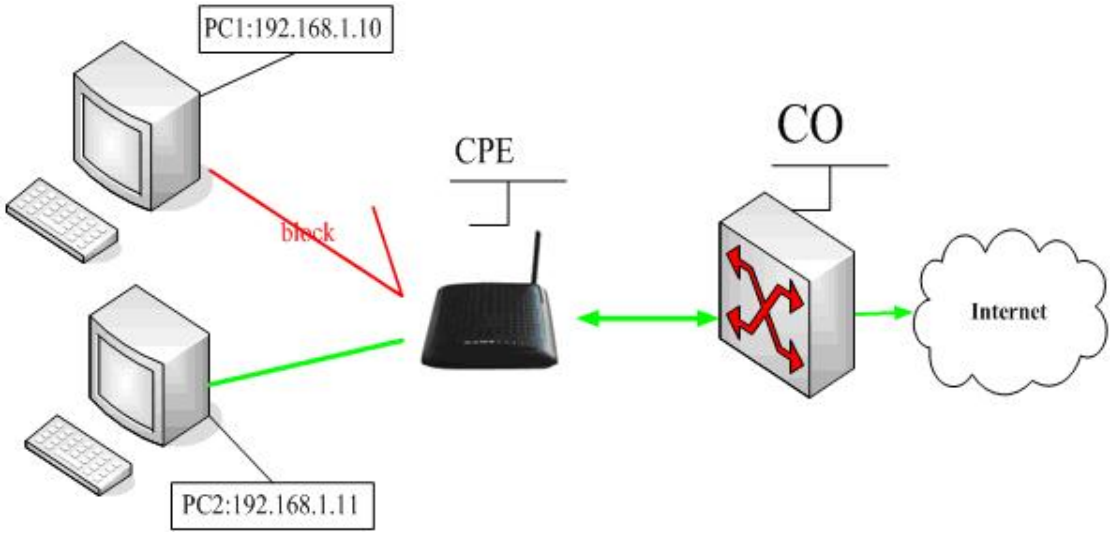


Figure2.8.6.9: Outgoing IP filer application

Request:

- I need to block a whose IP address is 192.168.1.10. All outgoing UDP/TCP packet from that PC1(192.168.1.10) is disallowed.
- Allow all outgoing traffic packet from PC2(192.168.1.11) .

Configuration:

Step1. By default, all outgoing IP traffic from LAN is allowed, so allow all the IP packet come for the PC2 .

Setp2.The detailed configuration steps are as follows:

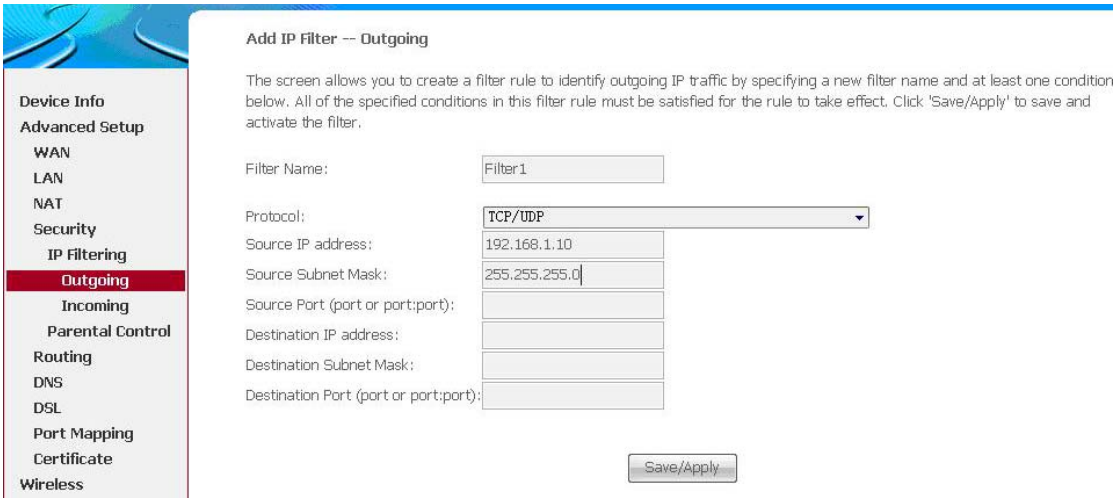


Figure2.8.6.10: Outgoing IP Filtering Add Setup example

Click “Save/apply” to show below.

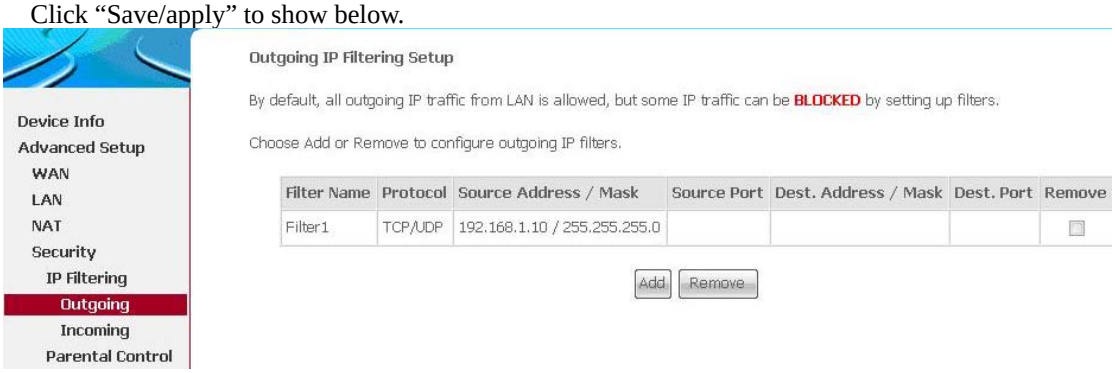


Figure2.8.7.1: Outgoing IP Filtering Config Complete

4.4.4.2 Incoming IP Filtering Setup

The incoming IP filter is used to block and permit IP packet transmisstion from internet. By default incoming IP filter block all incoming packet from internet. When incoming IP Filtering rules setup being enable on the MODEM, you can permit remote individual PC to access various local network service .

Click “Security”-->” IP Filtering”-->” Incoming” to show the following interface.
By default, all incoming IP traffic from the WAN is blocked when the firewall is enabled. However, some IP traffic can be ACCEPTED by setting up filters.

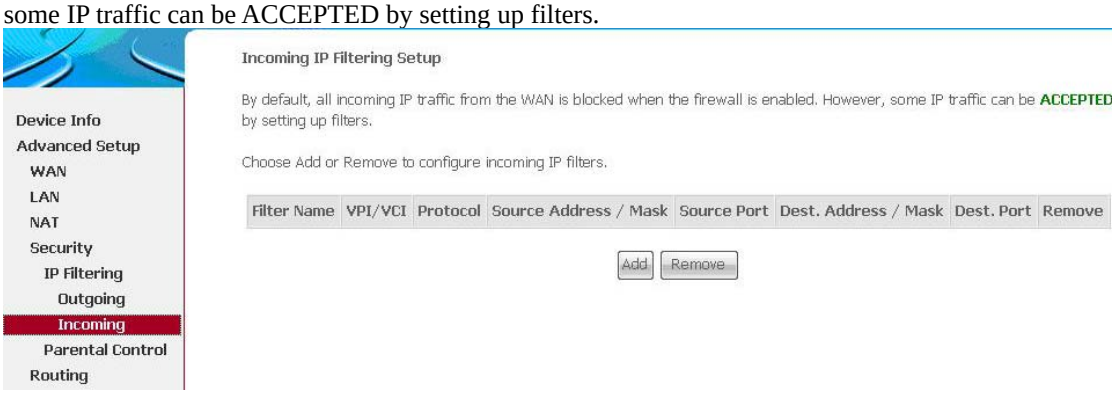


Figure2.8.7.2: Incoming IP Filtering Config

Click “Add” to enter the related interface defining the IP filtering rule as follows.
The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.

And you must select at least one or multiple WAN interfaces to apply this rule.

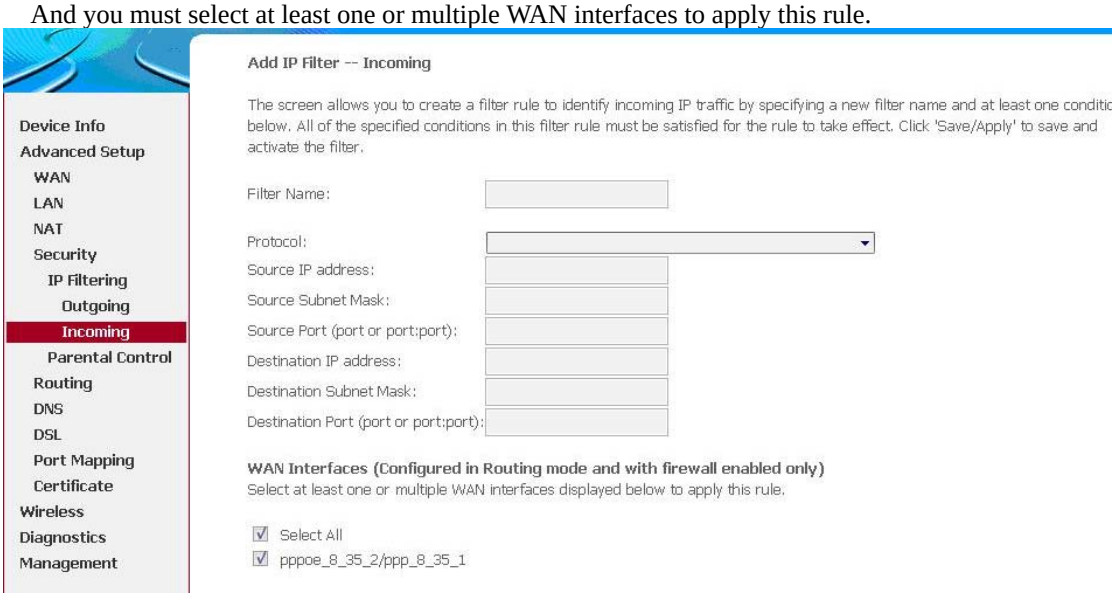


Figure2.8.7.3: Incoming IP Filtering Add Setup

. Filter Name: Enter the name of incoming filter rule
. Protocol: select one among TCP/UDP TCP UDP or ICMP protocols
. Source IP address: Enter a ip address. when you have set ip address ,the incoming packet (protocol selected packet) will allow.
Source subnet mask:
Source port : UPD/TCP source port or a range of ports
Destination IP address: destination ip (default no set)
Destination subnet mask:
Destination port : UPD/TCP destination port or a range of ports
Wan interfaces: You can select wan interfaces and PVC

There are a example to introduce how to configure the incoming IP Filtering:

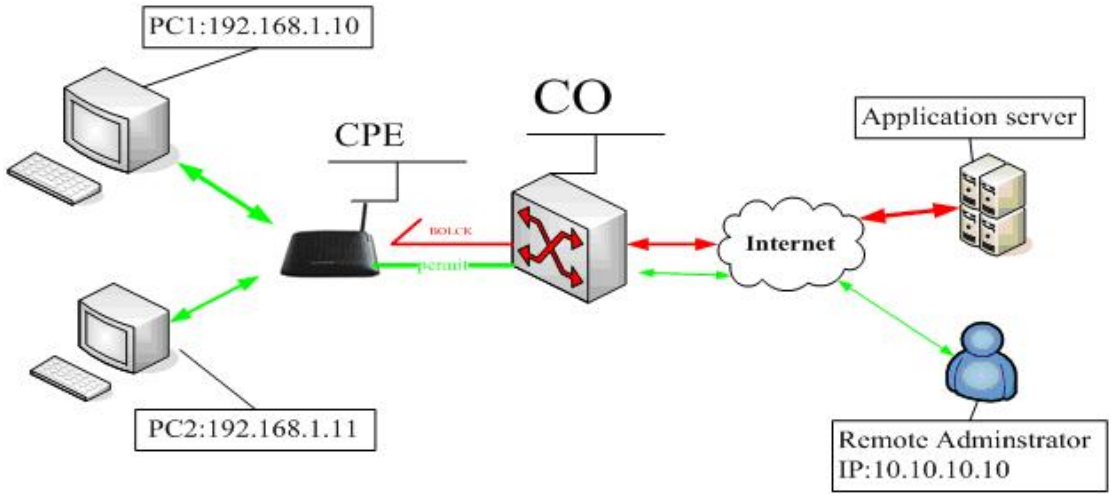


Figure 1.2 incoming IP filer application

Request:

- I need to permit a PC whose IP address is 10.10.10.10. All Incoming TCP/UDP packet traffic from that PC(10.10.10.10) is allowed.
- Block all IP traffic from other PC .

Step1. By default, all incoming IP traffic from internet is blocked, so all the IP packet come for the internet are blocked.

Setp2.

The detailed configuration steps are as follows:

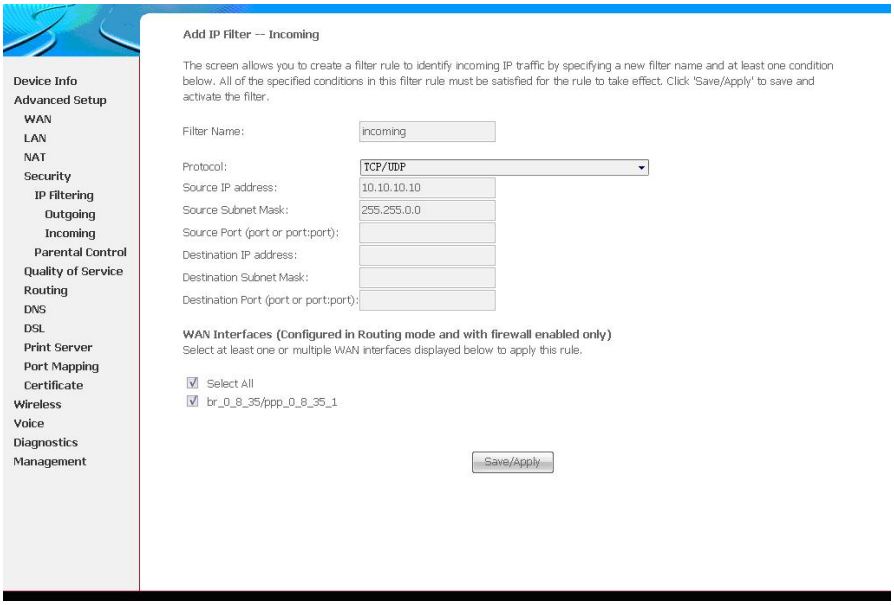

Add IP Filter -- Incoming
The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.
Filter Name: incoming
Protocol: TCP/UDP
Source IP address: 10.10.10.10
Source Subnet Mask: 255.255.0.0
Source Port (port or port:port):
Destination IP address:
Destination Subnet Mask:
Destination Port (port or port:port):
WAN Interfaces (Configured in Routing mode and with firewall enabled only)
Select at least one or multiple WAN interfaces displayed below to apply this rule.
Select All
br_0_8_35/ppp_0_8_35_1
Save/Apply
Device Info
Advanced Setup
WAN
LAN
NAT
Security
IP Filtering
Outgoing
Incoming
Parental Control
Quality of Service
Routing
DNS
DSL
Print Server
Port Mapping
Certificate
Wireless
Voice
Diagnostics
Management

Figure2.8.7.4: Incoming IP Filtering Add Setup example

Click “Save/apply” to show below.

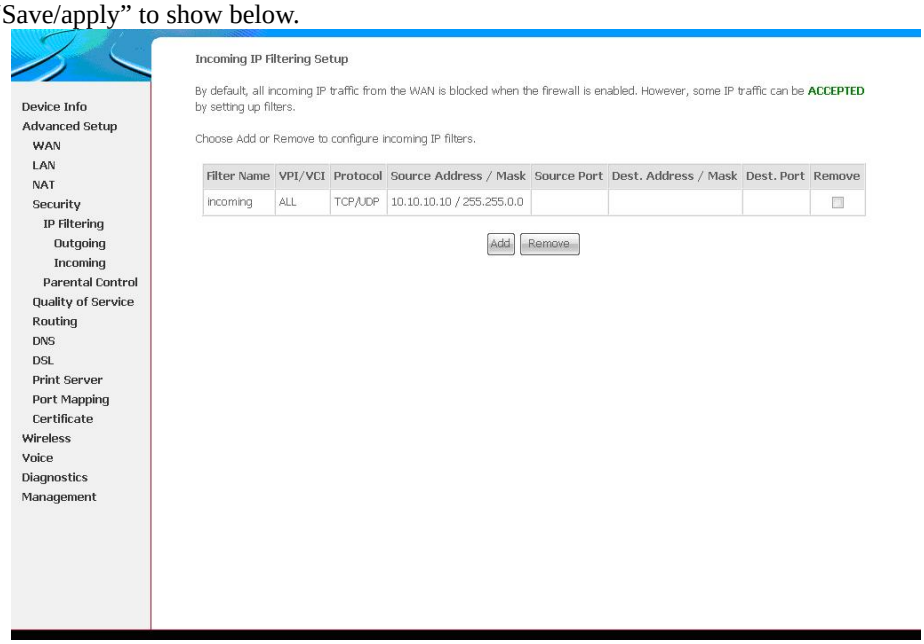


Figure2.8.7.5: Incoming IP Filtering Config Complete

4.4.4.3 MAC Filtering Setup

May be you want manage Layer 2 MAC address to block or permit a computer within the home network .when you enable MAC filter rules ,the MODEM serves as a firewall which work at layer 2. Click “Security”-->”MAC Filtering” to show the following interface.

Note: MAC Filtering is only effective on ATM PVCs configured in Bridge mode. If the ATM PVCs is configured in other routing mode(such as PPPoE mode), the “MAC Filtering Setup” will not appears in the “Security” option.

FORWARDED means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

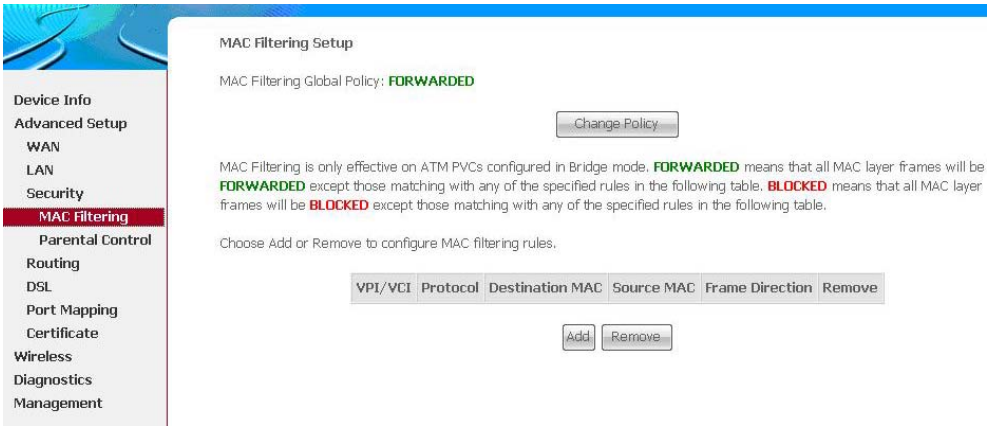

MAC Filtering Setup
MAC Filtering Global Policy: FORWARDED
Change Policy
MAC Filtering is only effective on ATM PVCs configured in Bridge mode. FORWARDED means that all MAC layer frames will be FORWARDED except those matching with any of the specified rules in the following table. BLOCKED means that all MAC layer frames will be BLOCKED except those matching with any of the specified rules in the following table.
Choose Add or Remove to configure MAC filtering rules.
VPI/VCI
Protocol
Destination MAC
Source MAC
Frame Direction
Remove
Add
Remove
Device Info
Advanced Setup
WAN
LAN
Security
MAC Filtering
Parental Control
Routing
DSL
Port Mapping
Certificate
Wireless
Diagnostics
Management

Figure2.8.7.6: MAC Filtering Setup overview

Click “Change Policy” to show the following interface. Then you can change the MAC Filtering Global Policy from FORWARDED to BLOCKED.

Change MAC Filtering Global Policy
WARNING: Changing from one global policy to another will cause all defined rules to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.
Are you sure you want to change MAC Filtering Global Policy from FORWARDED to BLOCKED ?
NO
YES
Device Info
Advanced Setup
WAN
LAN
Security
MAC Filtering
Parental Control
Routing
DSL
Port Mapping
Certificate

Figure2.8.7.7: MAC Filtering Change Policy

Click “add” to add MAC filter rules. The interface show below.

Figure2.8.7.8: MAC Filtering Add Config

Protocol Type: select one among PPPoE IPV4 IPV6 AppleTalk IPX NETBEUI or ICMP protocols
Destination MAC Address:
Source MAC Address :
Frame Direction : the direction of transmit frame,you can select LAN->WAN(from lan to wan) WAN -> LAN(from wan to lan) LAN ⇔ WAN.
WAN Interface : select a wan interface.

4.4.4.3.1 MAC Filtering -----Global Policy FORWARDED

Let me show you how to forbid the PC which has the 00:13:20:9E:0F:10 MAC address transmit PPPoE frame to internet..

Click “add” to configure as the interface below.

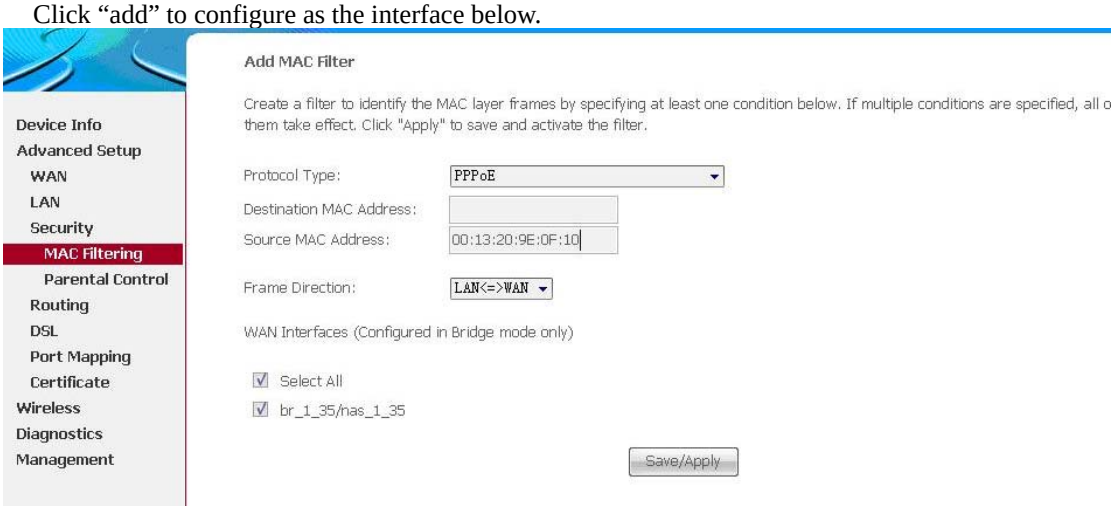


Figure2.8.7.9: MAC Filtering Add Config example

click “Save/Apply” to show below.

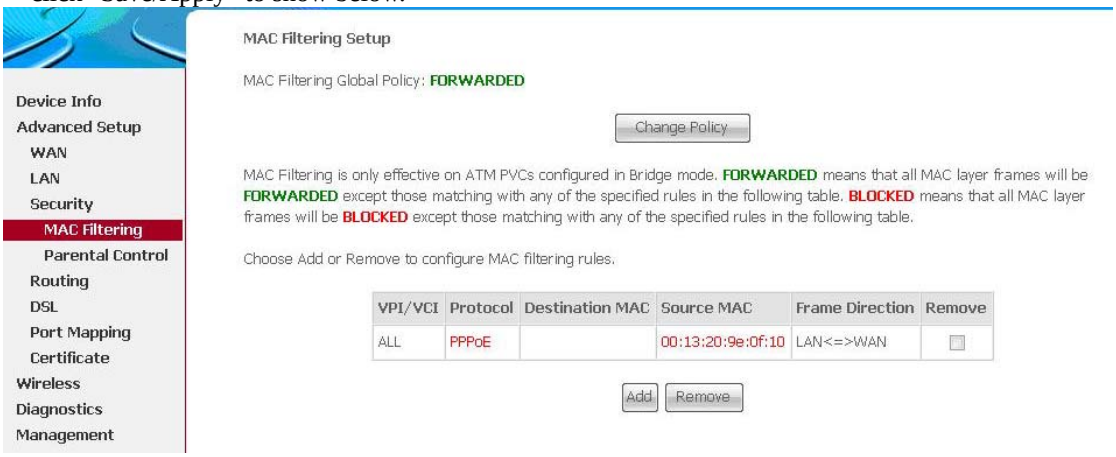

MAC Filtering Setup
MAC Filtering Global Policy: FORWARDED
Change Policy
MAC Filtering is only effective on ATM PVCs configured in Bridge mode. FORWARDED means that all MAC layer frames will be
FORWARDED except those matching with any of the specified rules in the following table. BLOCKED means that all MAC layer
frames will be BLOCKED except those matching with any of the specified rules in the following table.
Choose Add or Remove to configure MAC filtering rules.
VPI/VCI Protocol Destination MAC Source MAC Frame Direction Remove
ALL PPPoE 00:13:20:9e:0f:10 LAN<=>WAN
Add Remove
Device Info
Advanced Setup
WAN
LAN
Security
MAC Filtering
Parental Control
Routing
DSL
Port Mapping
Certificate
Wireless
Diagnostics
Management

Figure2.8.7.10: MAC Filtering Add Config Complete

4.4.4.3.2 MAC Filtering -----Global Policy BLOCKED

Let me show you how to permit the PC who has the 00:13:20:9E:0F:10 MAC address transmit PPPoE frame to internet.
Click “add” to configure as the interface below.

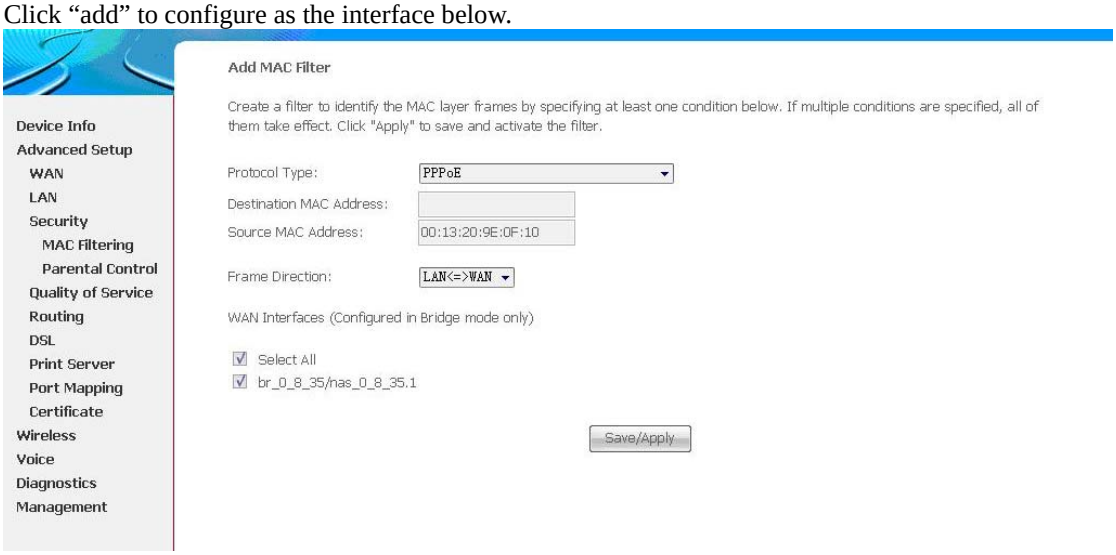


Figure2.8.8.1: MAC Filtering BLOCKED Add Config

click “Save/Apply” to show below.

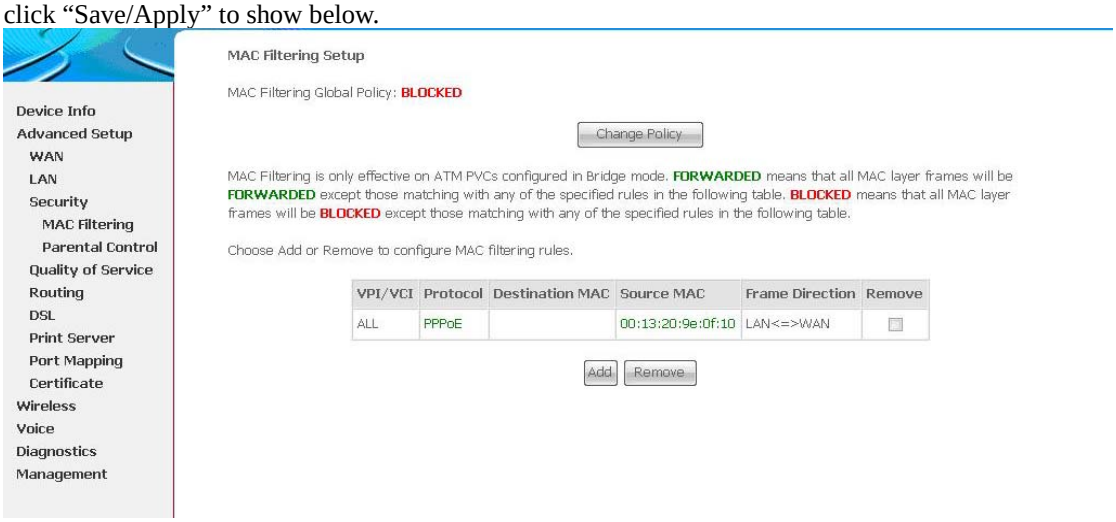


Figure2.8.8.2: MAC Filtering BLOCKED Add Config Complete

4.4.5 Quality of Service

Many communication and multimedia applications require large, high speed bandwidths to transfer data between the local network and the internet. However ,for many applications there is often only one internet connection available with limited capacity. QOS(Quality of Service)divides this capacity between the different applications and provides underlayed, continuous data transfer where data packets with higher priority are given preference.

Click “Quality of Service” to show the following interface. Under “Quality of Servcie ”,there are two network share mode: ”Queue Config”, ”Qos Classification”.

Quality of Service (QoS) for networks is an industry-wide set of standards and mechanisms for ensuring high-quality performance for critical applications. By using QoS mechanisms, network administrators can use existing resources efficiently and ensure the required level of service without reactively expanding or over-provisioning their networks.

Traditionally, the concept of quality in networks meant that all network traffic was treated equally. The result was that all network traffic received the network’s best effort, with no guarantees for reliability, delay, variation in delay, or other performance characteristics. With best-effort delivery service, however, a single bandwidth-intensive application can result in poor or unacceptable performance for all applications. The QoS concept of quality is one in which the requirements of some applications and users are more critical than others, which means that some traffic needs preferential treatment.

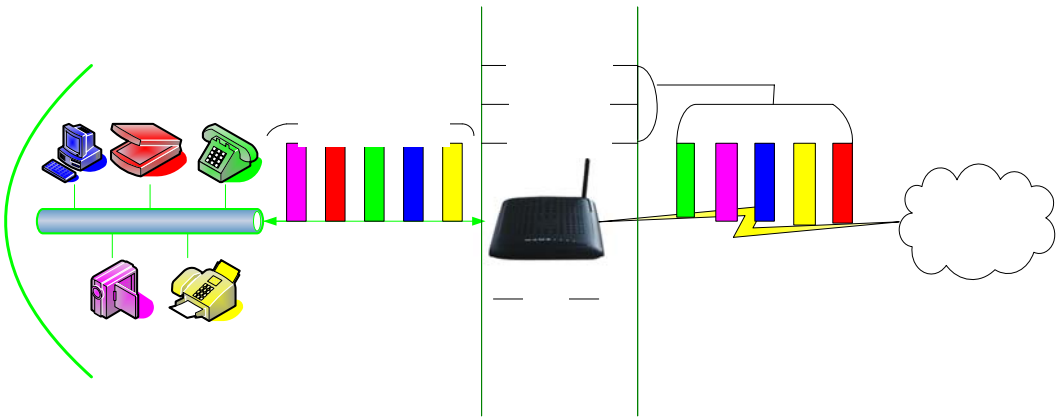


Figure 4.4.5 Quality of Service

4.4.5.1 Enable QOS

In this interface, you can do QOS queue management configuration. By default ,the system is enable QOS and set a default DSCP mark to automatically mark incoming traffic without reference to particular classifier.
Click ”Advance Setup”→”Quality of Classification” to show following interface:

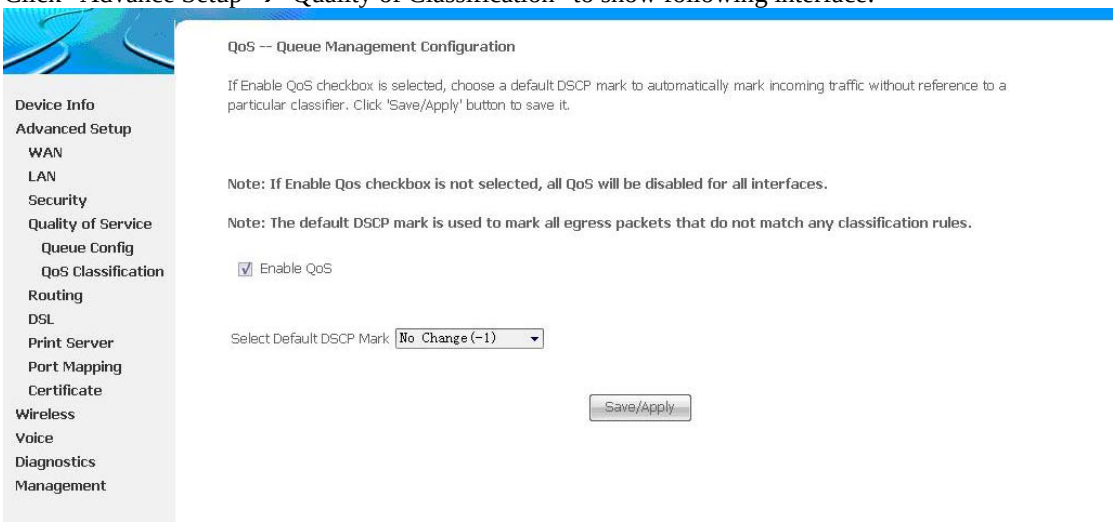

QoS -- Queue Management Configuration
If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Save/Apply' button to save it.
Note: If Enable Qos checkbox is not selected, all QoS will be disabled for all interfaces.
Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.
Enable QoS
Select Default DSCP Mark
No Change(-1)
Save/Apply
Device Info
Advanced Setup
WAN
LAN
Security
Quality of Service
Queue Config
QoS Classification
Routing
DSL
Print Server
Port Mapping
Certificate
Wireless
Voice
Diagnostics
Management

Figure2.8.8.3: QOS queue management configuration

Choose “Enable QOS” can enable QOS and the system can set default DSCP mark
Click “save/Apply”to active QOS.

4.4.5.2 QOS--Queue Config

The queueing in packet QOS will become effective only when packet is forwarded to QoS-enabled PVC. Packet forwarding is determined by IP routing or bridging , not under control of the packet Qos.
Click “Queue Config” to pop up an interface as below. In this interface , you can config QOS Queue. A maximum 24 entries can be configured.
Qos Queue Configuration can allocated three queues .Each of the queues can be configured for a precedence value(Lower integer values for precedence imply higher priority for this queue relative to others). The queue entry configured here will be used by the classifier to place ingress packets appropriately.

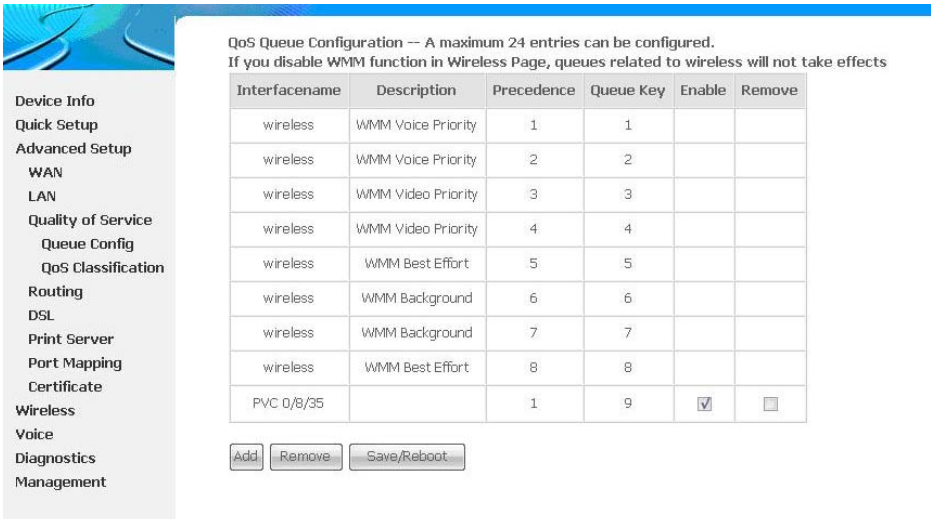

QoS Queue Configuration -- A maximum 24 entries can be configured.
If you disable WMM function in Wireless Page, queues related to wireless will not take effects
Interfacename | Description | Precedence | Queue Key | Enable | Remove
wireless | WMM Voice Priority | 1 | 1
wireless | WMM Voice Priority | 2 | 2
wireless | WMM Video Priority | 3 | 3
wireless | WMM Video Priority | 4 | 4
wireless | WMM Best Effort | 5 | 5
wireless | WMM Background | 6 | 6
wireless | WMM Background | 7 | 7
wireless | WMM Best Effort | 8 | 8
PVC 0/8/35 | | 1 | 9
Add
Remove
Save/Reboot
Device Info
Quick Setup
Advanced Setup
WAN
LAN
Quality of Service
Queue Config
QoS Classification
Routing
DSL
Print Server
Port Mapping
Certificate
Wireless
Voice
Diagnostics
Management

Figure2.8.8.4:QoS Queue Config overview

NOTE: Lower integer values for precedence imply higher priority for this queue relative to others.
For exampe: add a Qos queue entry and allocate it to a specific network interface(PVC 0/8/81)。Set

integer values for queue precedence is 2.

Step 1. Click “add ” bottom to show following interface:

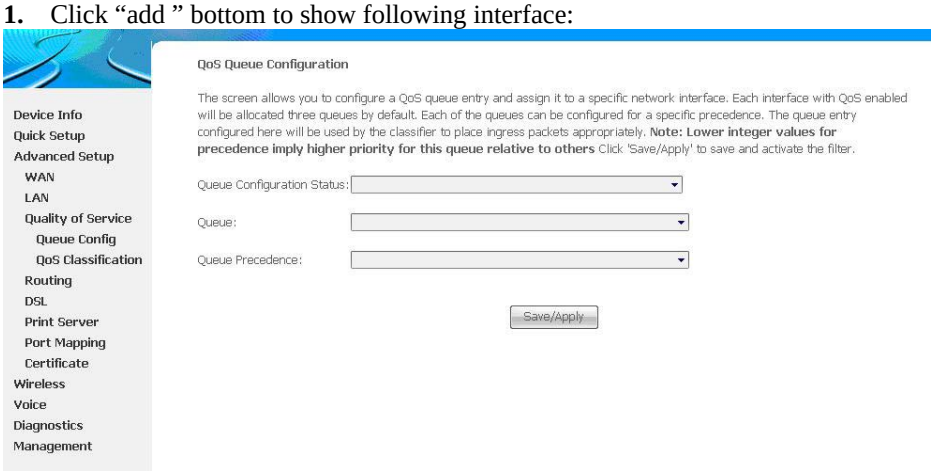

QoS Queue Configuration
The screen allows you to configure a QoS queue entry and assign it to a specific network interface. Each interface with QoS enabled will be allocated three queues by default. Each of the queues can be configured for a specific precedence. The queue entry configured here will be used by the classifier to place ingress packets appropriately. Note: Lower integer values for precedence imply higher priority for this queue relative to others Click 'Save/Apply' to save and activate the filter.
Queue Configuration Status:
Queue:
Queue Precedence:
Save/Apply
Device Info
Quick Setup
Advanced Setup
WAN
LAN
Quality of Service
Queue Config
QoS Classification
Routing
DSL
Print Server
Port Mapping
Certificate
Wireless
Voice
Diagnostics
Management

Figure2.8.8.5: QoS Queue Config

Queue Configuration Status:Enable or Disable to configure a Qos queue entry.
Queue : select a specific network interface.When you have already selected a network interface ,the specific network interface selected will automatically allocate to the queue
Queue Precedence : select a integer value for queue precedence. when you have already selected a integer value, the queue entry will place to ingress packets apporiately. Lower integer values for precedence imply higher priority for this queue relative to others.

Step2: add a Qos queue entry and assign it to a specific network interface(PVC 0/8/81),set integer values for queue precedence is 2. Show following interface:

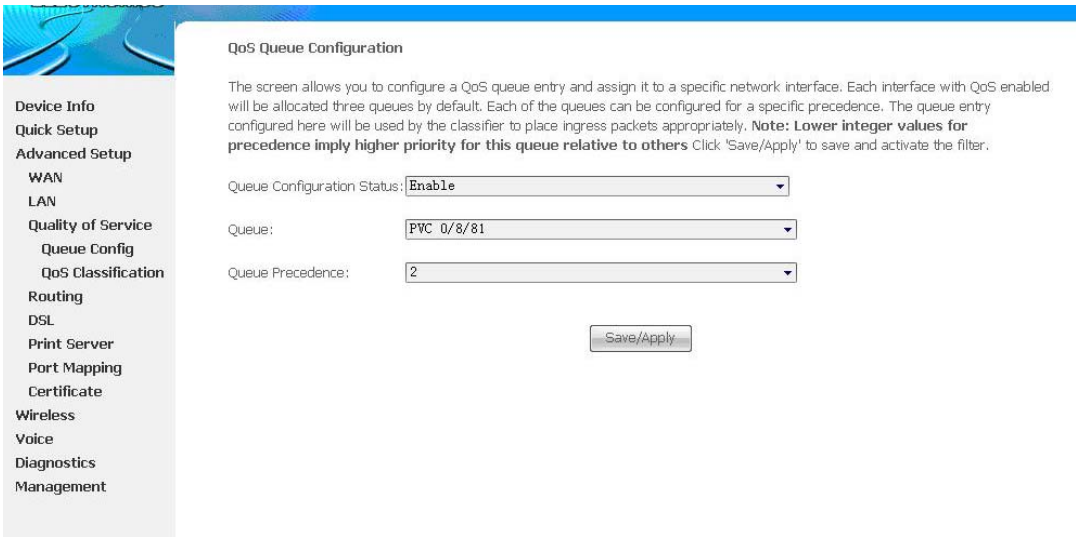

QoS Queue Configuration
The screen allows you to configure a QoS queue entry and assign it to a specific network interface. Each interface with QoS enabled will be allocated three queues by default. Each of the queues can be configured for a specific precedence. The queue entry configured here will be used by the classifier to place ingress packets appropriately. Note: Lower integer values for precedence imply higher priority for this queue relative to others Click 'Save/Apply' to save and activate the filter.
Queue Configuration Status: Enable
Queue: PVC 0/8/81
Queue Precedence: 2
Save/Apply
Device Info
Quick Setup
Advanced Setup
WAN
LAN
Quality of Service
Queue Config
QoS Classification
Routing
DSL
Print Server
Port Mapping
Certificate
Wireless
Voice
Diagnostics
Management

Figure2.8.8.6: QoS Queue Config example

After proper modifications, click “Save/Apply” to show the following interface. (This configuration will take effective at once.)

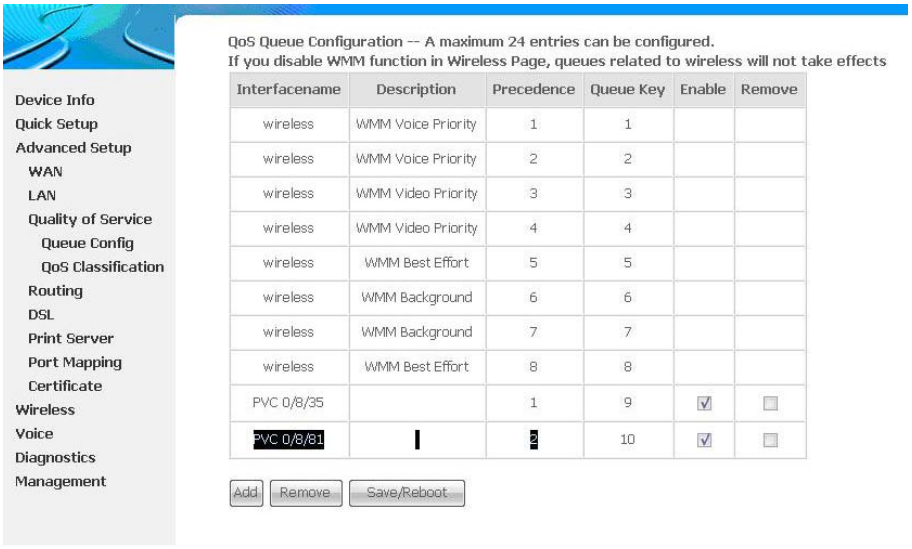


Figure2.8.8.7: QoS Queue Config Complete

If you want to delete a certain queue,you can disable this queue and choose this queue ,last click "Remove" botton to delete it.
After the queue config is already configured, you can creates serval traffic class rule to classify the upstream traffic.

4.4.5.3 QoS--QoS Classification

Some application require that specific bandwiths ensure its data be forward in the time.Qos classification can creates traffic class rule to classify the upstream traffic. Assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte .After Qos classification, Qos divides capacity between the different applications and provides undelayed ,continuous data transfer where data packet with higher priority are given preference. The follow diagram show how Qos classify the

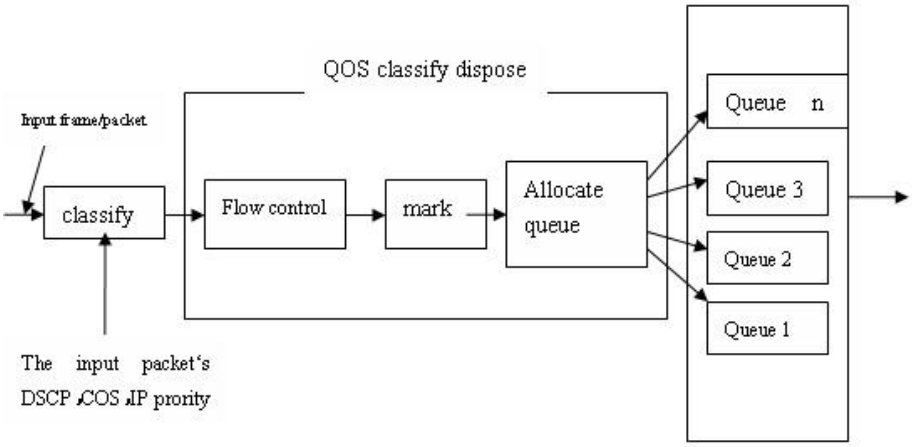


Figure 1.1 name picture

Click "Qos Classification" to pop up an interface as below. In this interface ,you can configure network traffic classes.

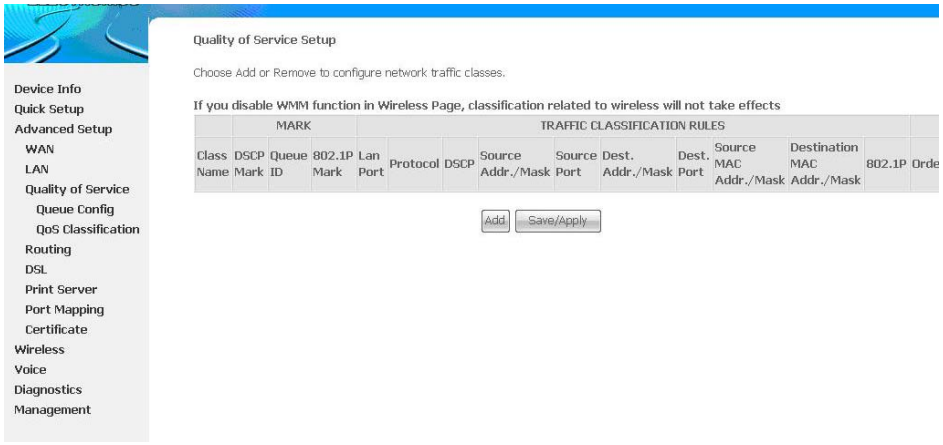


Figure2.8.8.8: Qos Classification Conifg overview

Click “Add” to show the following interface.

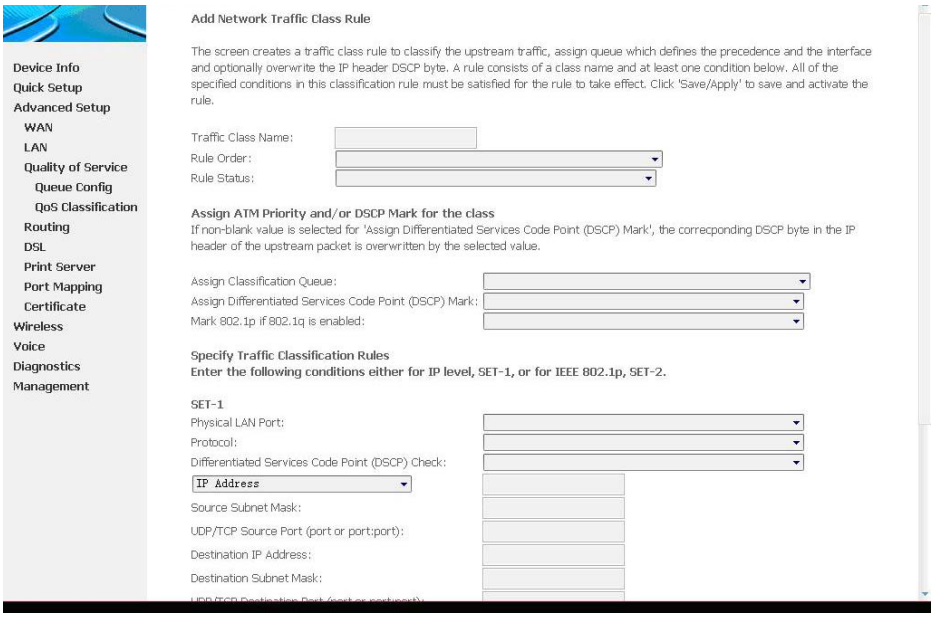

Add Network Traffic Class Rule
The screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the rule.
Traffic Class Name:
Rule Order:
Rule Status:
Assign ATM Priority and/or DSCP Mark for the class
If non-blank value is selected for 'Assign Differentiated Services Code Point (DSCP) Mark', the correcponding DSCP byte in the IP header of the upstream packet is overwritten by the selected value.
Assign Classification Queue:
Assign Differentiated Services Code Point (DSCP) Mark:
Mark 802.1p if 802.1q is enabled:
Specify Traffic Classification Rules
Enter the following conditions either for IP level, SET-1, or for IEEE 802.1p, SET-2.
SET-1
Physical LAN Port:
Protocol:
Differentiated Services Code Point (DSCP) Check:
IP Address
Source Subnet Mask:
UDP/TCP Source Port (port or port:port):
Destination IP Address:
Destination Subnet Mask:
Device Info
Quick Setup
Advanced Setup
WAN
LAN
Quality of Service
Queue Config
QoS Classification
Routing
DSL
Print Server
Port Mapping
Certificate
Wireless
Voice
Diagnostics
Management

Figure2.8.8.9: Qos Classification Conifg

Traffic Class Name: Enter a name of the class
Rule Order: select order for queue
Rule Status: Enable or disable this traffic class rule
Assign Classfication Queue: select a classification queue
Assign Differentiated Service Code Point(DSCP)Mark: select a mark service that will modify the original packet IP header if all the rules defined within the classification class are matched .(CS ---Mark IP Precedence AF----Assured Forwarding EF---Expedited Forwarding)
Mark 802.1p if 802.1q is enabled: select a 802.1p priority number that will serve as the 802.1p value.

There are two sets of classification rules. Set-1 is based on different fields within TCP/UDP/IP layer plus physical LAN port; Set-2 is based on MAC layer IEEE 802.1p priority field.

Set-1 Rules contain the following

Physical LAN port: select one among usb port ,Ethernet ports and wireless port
Protocol: select one among TCP/UDP TCP UDP or ICMP protocols
Source IP address
Source subnet mask
UPD/TCP source port or a range of ports
Destination IP address
Destination subnet mask
UPD/TCP destination port or a range of ports

Source Mac address
Source Mac mask
Destination Mac address
Destination Mac Mask

Set-2 Rules contain the following:

802.1p priority:The 802.1p header includes a 3-bit prioritization field , which allows packets to be grouped into eight levels of priority(0-7), where level 7 is the highest one.

4.4.5.3.1 Qos--DSCP setting

In order to understand what is Differentiated Services Code Point(DSCP),one must first be familiarized with the Differentiated Services model.

Differentiated Services (Diffserv) is a Class of Service(COS)model that enhances best-effort Internet services by differentiating traffic by users , service requirements and other criteria. Packets are specifically marked, allowing network nodes to provide different levels of service,

Via priority queuing or bandwidth allocation, or by choosing dedicated routes for specific traffic flows.

Display by follow diagram. In the IPV4 packet have a TOS filed . Diffserv defines TOS field in IP packet headers refered to as DSCP. Hosts or routes passing traffic to a Diffserv-enabled network will typically mark each transmitted packet with an appropriate DSCP. The DSCP markings are used by Diffserv network routers to appropriately calssify packets and to apply particular queue handing or scheduling behavior.

Layer 3 IPV4 packet

Version /length	TOS （1word）	length	ID	Offset /mark	TTL	protocol	Check sum	IP-SA	IP-DA	data

TOS filed-----IP prority（TOS front 3 bit） or DSCP（front 6 bit）

7	6	5	4	3	2	1	0
IP prority			undefined				
DSCP						Flow control	

For example: marking each transmitted ICMP packet which passing traffic to 8-81class with an appropriate DSCP (CS5) . After set in the following interface :

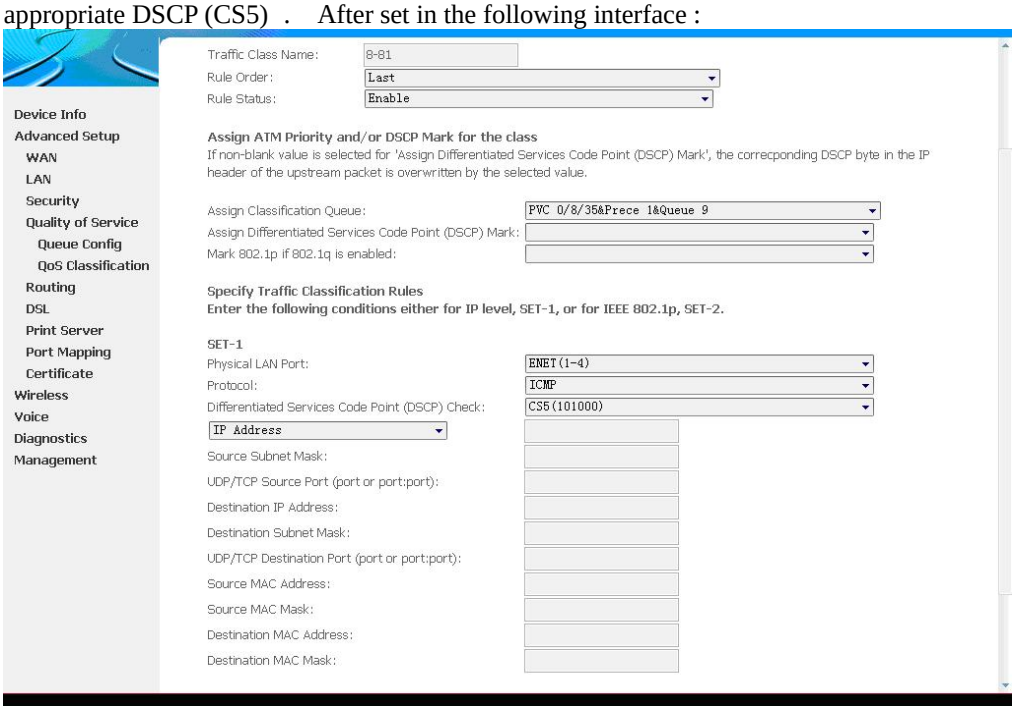

Device Info
Advanced Setup
WAN
LAN
Security
Quality of Service
Queue Config
QoS Classification
Routing
DSL
Print Server
Port Mapping
Certificate
Wireless
Voice
Diagnostics
Management
Traffic Class Name: 8-81
Rule Order: Last
Rule Status: Enable
Assign ATM Priority and/or DSCP Mark for the class
If non-blank value is selected for 'Assign Differentiated Services Code Point (DSCP) Mark', the correcponding DSCP byte in the IP header of the upstream packet is overwritten by the selected value.
Assign Classification Queue: PVC 0/8/35&Prece 1&Queue 9
Assign Differentiated Services Code Point (DSCP) Mark:
Mark 802.1p if 802.1q is enabled:
Specify Traffic Classification Rules
Enter the following conditions either for IP level, SET-1, or for IEEE 802.1p, SET-2.
SET-1
Physical LAN Port: ENET(1-4)
Protocol: ICMP
Differentiated Services Code Point (DSCP) Check: CS5(101000)
IP Address
Source Subnet Mask:
UDP/TCP Source Port (port or port:port):
Destination IP Address:
Destination Subnet Mask:
UDP/TCP Destination Port (port or port:port):
Source MAC Address:
Source MAC Mask:
Destination MAC Address:
Destination MAC Mask:

Figure2.8.8.10: Qos DSCP setting Conifg example

After proper modifications, click “Save/Apply” to show the following interface.

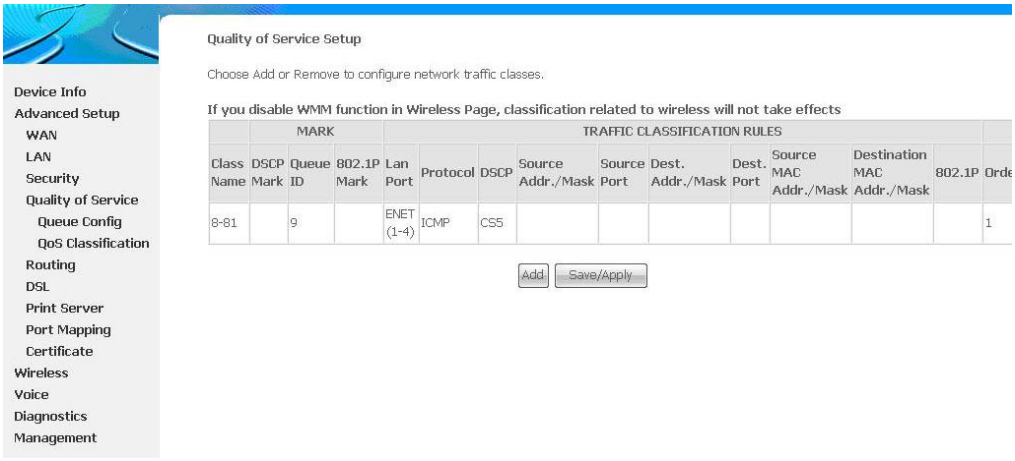


Figure2.8.9.1Qos Classification Conifg Complete

click “Save/Apply”.(This configuration will take effective at once.)

4.4.5.3.2 Qos--802.1p setting

The IEEE802.1p priority marking method is a standard for prioritizing network traffic at the data link/Mac sub-layer 802.1p traffic is simply classified and sent to the destination, with no bandwidth reservations established.

The follow diagram show the structure of 802.1Q Frame. The 802.1Q header includes a 3-bit prioritization field, which allows packets to be grouped to be grouped into eight levels of priority(0-7) ,where level 7 is the highest one. In addition , DSL maps these eight levels to priority queues , where queue 1 has the highest priority.

Layer 2 802.Q frame

Preamble	SFD	DA	SA	mark（4 word）	Len/Etype（2word）	DATA	FCS

mark：

TPID(0x8100)	Priority(3bit)	CFI（1bit）	VLAN ID(12bit)

For example: Mark the frame of 802.1p that queued to Queue 9 on vlaue 2. After set in the following interface :

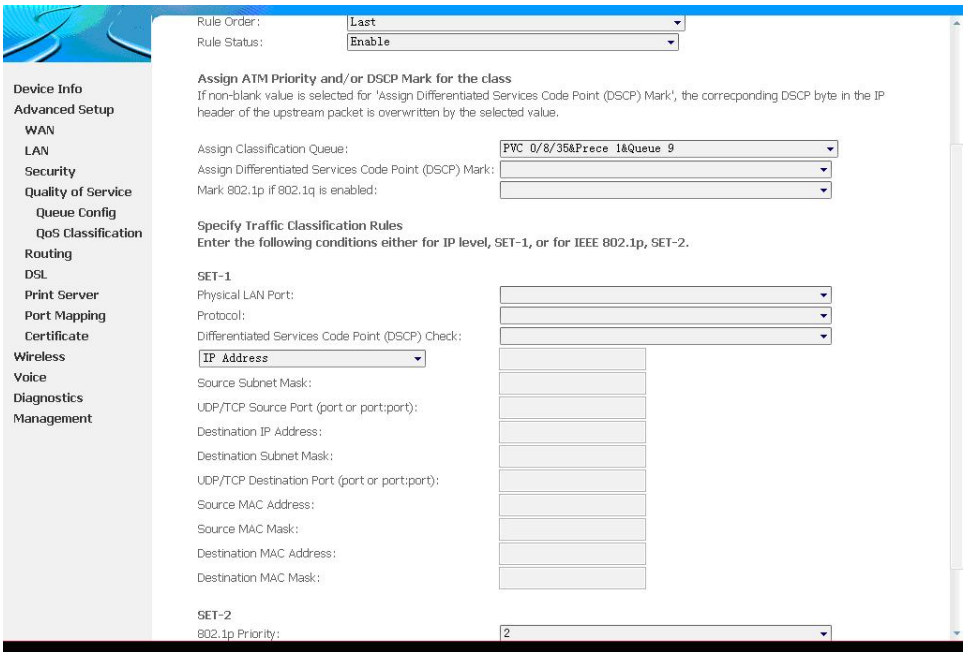


Figure2.8.9.2:QoS 802.1p setting

After proper modifications, click “Save/Apply” to show the following interface.

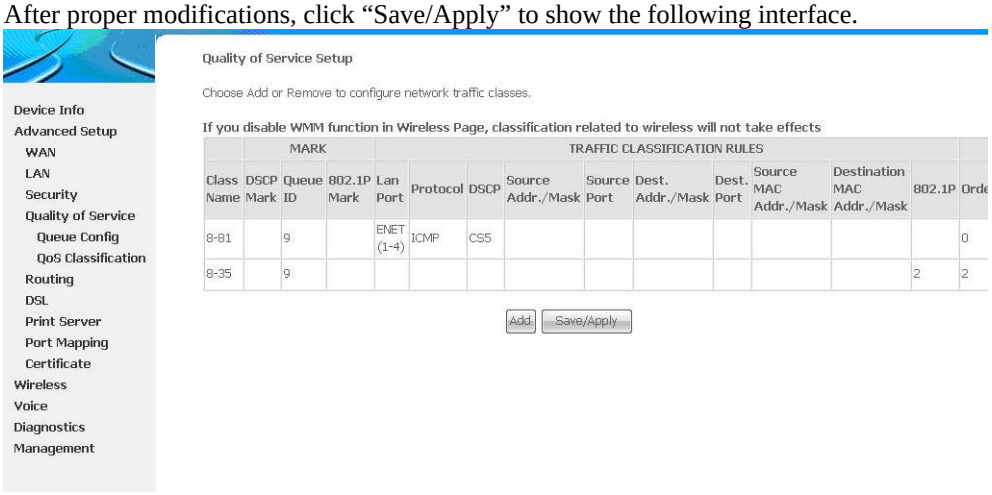


Figure2.8.9.3: :QoS 802.1p setting Complete

click “Save/Apply”.(This configuration will take effective at once.)

4.4.6 Routing

4.4.6.1 Routing – Default Gateway

In this interface, you can modify the Default Gateway settings.

If Enable Automatic Assigned Default Gateway checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway AND/OR a WAN interface. Click 'Save/Apply' button to save it.

NOTE:
If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the router to get the automatic assigned default gateway.

- If you want to use a default gateway, please click “ENABLE Automactic Assigned DefaultGateway” box to show the following interface.

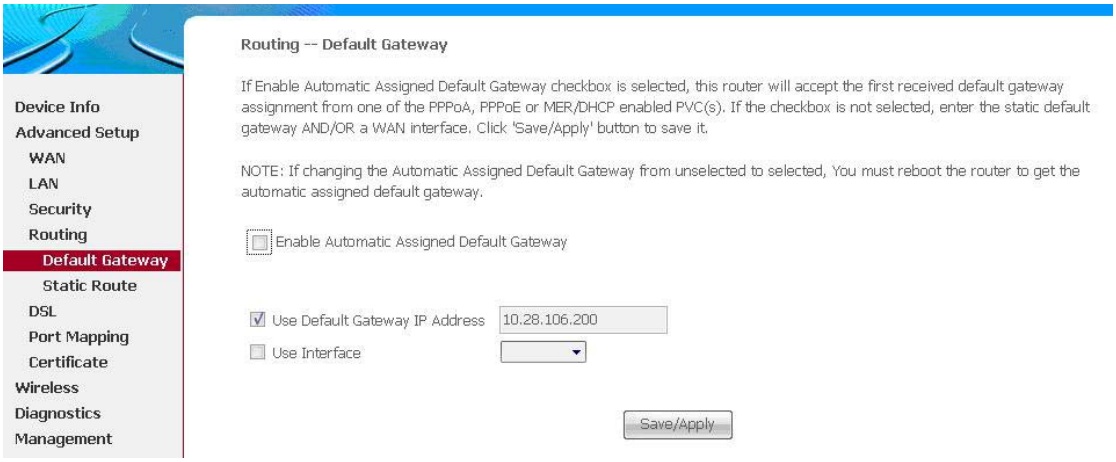

Routing -- Default Gateway
If Enable Automatic Assigned Default Gateway checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway AND/OR a WAN interface. Click 'Save/Apply' button to save it.
NOTE: If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the router to get the automatic assigned default gateway.
Enable Automatic Assigned Default Gateway
Use Default Gateway IP Address
10.28.106.200
Use Interface
Save/Apply
Device Info
Advanced Setup
WAN
LAN
Security
Routing
Default Gateway
Static Route
DSL
Port Mapping
Certificate
Wireless
Diagnostics
Management

Figure2.8.9.4: Default Gateway

Use Default Gateway

- Select “Enable automatic Assigned Default Gateway” box

Custom DSL router Default Gateway

- Close “Enable automatic Assigned Default Gateway” box

- Entry Use Default Gateway IP Address
- Entry Use Interface: The interface that the packets pass through on the MODEM.
- Apply setting by click Save/Apply

4.4.6.2 Static Routes

Networking devices forward packets using route information that is either manually configured or dynamically learned using a routing protocol. Static routes are manually configured and define an explicit path between two networking devices. Unlike a dynamic routing protocol, static routes are not automatically updated and must be manually reconfigured if the network topology changes. The benefits of using static routes include security and resource efficiency. Static routes use less bandwidth than dynamic routing protocols and no CPU cycles are used to calculate and communicate routes. The main disadvantage to using static routes is the lack of automatic reconfiguration if the network topology changes.

Static routes can be redistributed into dynamic routing protocols but routes generated by dynamic routing protocols cannot be redistributed into the static routing table. No algorithm exists to prevent the configuration of routing loops that use static routes.

Static routes are useful for smaller networks with only one path to an outside network and to provide security for a larger network for certain types of traffic or links to other networks that need more control. In general, most networks use dynamic routing protocols to communicate between networking devices but may have one or two static routes configured for special cases

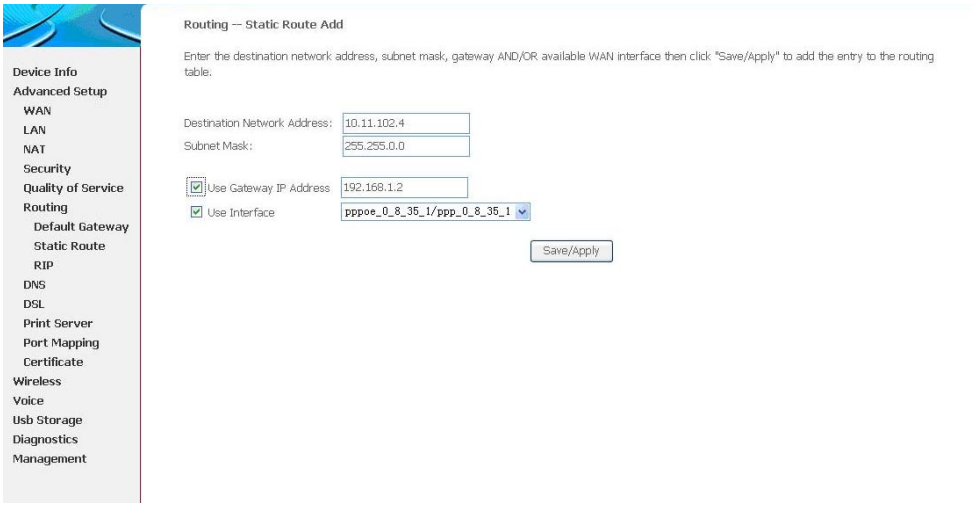


Figure2.8.9.5: Static routes Add Config

Add static route

- Entry destination network address
- Entry subtnet Mask
- Enable “Use Gateway IP Address” and entry IP address
- Select use interface
- Apply setting by click Save/Apply

Remove static route

- Select “remove” box on table
- Apply setting by click “remove”

4.4.6.3 RIP

4.4.6.3.1 Background

The Routing Information Protocol, or RIP, as it is more commonly called, is one of the most enduring of all routing protocols. RIP is also one of the more easily confused protocols because a variety of RIP-like routing protocols proliferated, some of which even used
the same name! RIP and the myriad RIP-like protocols were based on the same set of algorithms that use distance vectors to mathematically compare routes to identify the best path to any given destination address. These algorithms emerged from academic research that dates back to 1957. Today's open standard version of RIP, sometimes referred to as IP RIP, is formally defined in two documents: Request For Comments (RFC) 1058 and Internet Standard (STD) 56. As IP-based networks became both more numerous and greater in size, it became apparent to the Internet Engineering Task Force (IETF) that RIP needed to be updated. Consequently, the IETF released RFC 1388 in January 1993, which was then superceded in November 1994 by RFC 1723, which describes RIP 2 (the second version of RIP). These RFCs described an extension of RIP's capabilities but did not attempt to obsolete the previous version of RIP. RIP 2 enabled RIP messages to carry more information, which permitted the use of a simple authentication mechanism to secure table updates. More importantly, RIP 2 supported subnet masks, a critical feature that was not available in RIP.

This chapter summarizes the basic capabilities and features associated with RIP. Topics include the routing update process, RIP routing metrics, routing stability, and routing timers.

4.4.6.3.2 Routing Updates

RIP sends routing-update messages at regular intervals and when the network topology changes. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. The metric value for the path is increased by 1, and the sender is indicated as the next hop. RIP routers maintain only the best route (the route with the lowest metric value) to a destination. After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers of the change. These updates are sent independently of the regularly scheduled updates that RIP routers send

4.4.6.3.3 RIP Routing Metric

RIP uses a single routing metric (hop count) to measure the distance between the source and a destination network. Each hop in a path from source to destination is assigned a hop count value, which is typically 1. When a router receives a routing update that contains a new or changed destination network entry, the router adds 1 to the metric value indicated in the update and enters the network in the routing table. The IP address of the sender is used as the next hop

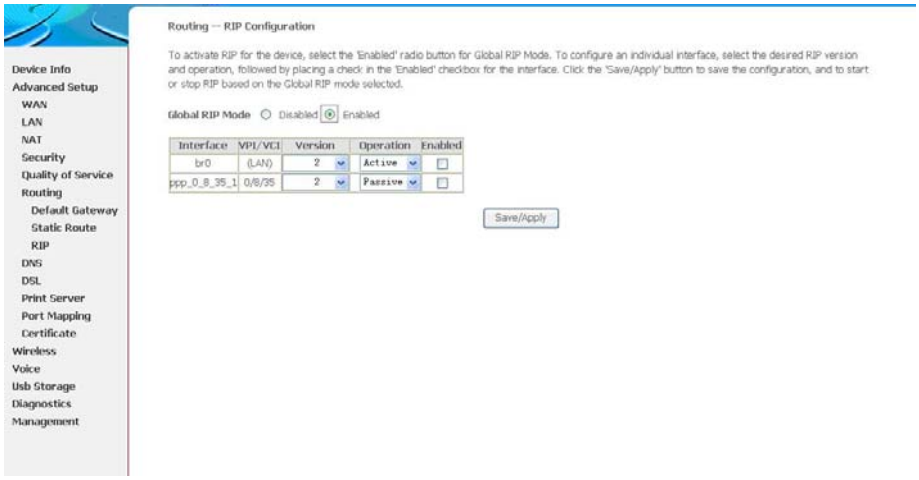

Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Routing
Default Gateway
Static Route
RIP
DNS
DSL
Print Server
Port Mapping
Certificate
Wireless
Voice
Usb Storage
Diagnostics
Management
Routing -- RIP Configuration
To activate RIP for the device, select the 'Enabled' radio button for Global RIP Mode. To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the 'Enabled' checkbox for the interface. Click the 'Save/Apply' button to save the configuration, and to start or stop RIP based on the Global RIP mode selected.
Global RIP Mode Disabled Enabled
Interface VPI/VCI Version Operation Enabled
br0 (LAN) 2 Active
ppp_0_8_35_1 0/8/35 2 Passive
Save/Apply

Figure2.8.9.6：RIP Configuration

4.4.6.3.4 RIP configuration

- To activate RIP for the device, select the 'Enabled' radio button for Global RIP Mode.
- To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the 'Enabled' checkbox for the interface.

Click the 'Save/Apply' button to save the configuration, and to start or stop RIP based on the Global RIP mode selected.

4.4.6.4 Policy Route

In this the Policy is that route IP packet base on the rule defined by network administrator. As a example, we can define the policy that the packets from network A, sended out from path X, the others sended out from path Y, or that the packets' s TOS value is A, sended out from path F, the others sended out from path K.

The policy route is introduced into the linux form the version 2.1 kernel. When compare with tradition route arithmetic, the policy route mainly introduced the concept of multi route table and rule.

4.4.6.4.1 Multi route table

The tradition route arithmetic use only one route table. For some cese, we need use multi route table. Suppose the subnet connect with internet by a router that is of two lines, the one line is of fast speed, the other line is of slow speed. Lost of users in the subnet have no special requirement for the speed, so they could use the slow line. but some special users have rigor requirement for the speed, so they must use the fast line. If we use one route table, it can't reach the aim. Route data packet base on sourec address or other parameter, use mutl route table for mutli user's requirement, so it can boost the router's performance.

4.4.6.4.2 Rule

Rule is the key concept in the policy route, we can describe rule use nation language, as a example, we can specify these rule:

Rule one: All the packets from 192.16.152.24, use route table 10, the PRI is 1500

Rule two: All the packets use route table 253, the PRI is 32767

We can know that the rule contain three element:

Which packet would apply such rule

What action would be adopt for the packet accord with such rule, as use which table.

Which PRI of such rule, higher PRI's rule prior match (the value more little the PRI more highter)

4.4.6.4.3 Principle

The policy route provided in the release 3.10L02 mainly bind the lan interface whih wan interface, just the packet come in from one lan interface can be transmit from one PVC by specify.

First at the second layer, use ebtables mark the packet come in from lan interface, then at the third layer use iproute select route path base on the mark.

Warning: thr PRI of the policy route is higher whih static route and rip route.

4.4.6.4.4 Configure

Before config policy route , need enbale port mapping fuction, after enable port mapping function, select the menuitem "Advanced Setup","Routing","Policy Route" in turn，will display the page as figure 1：

Figure1: the confige page of policy route

Click the button “add” , will display the page as figure 2：

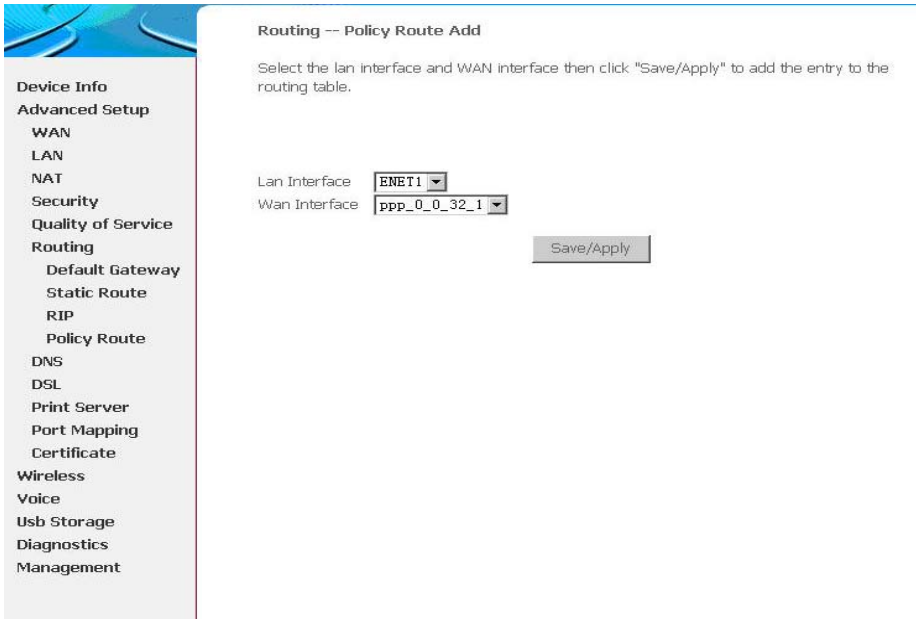


figure 2: the add page of policy route

- The Lan interface have four option, ENET1present the first lan interface , ENET2 present the second lan interface， analogy in turn, ENET4 present the fourth lan interface。
- The Wan interface is the route PVC configed by user, contain PPPOE, PPPOA, MER, IPOA etc.
- Select the lan interface and wan interface, click button ”save/apply”, save configure, as figure 3：

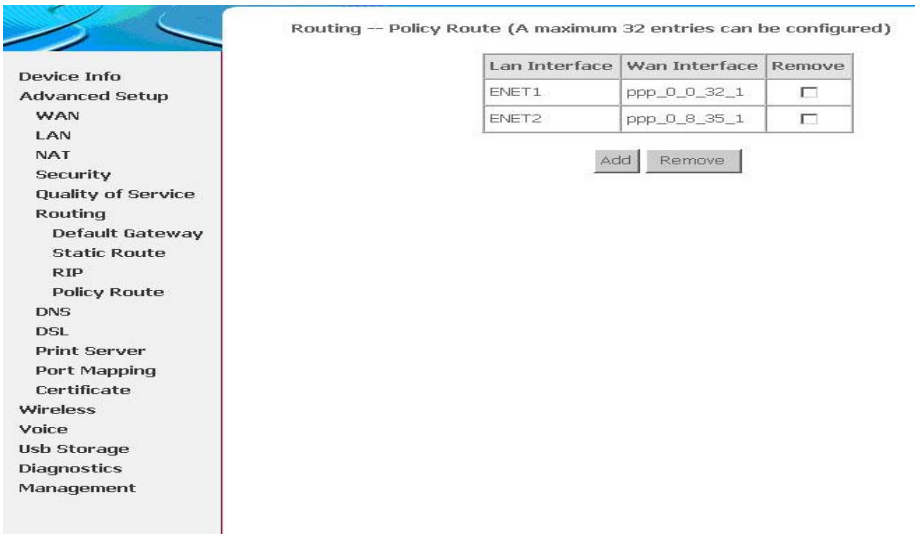


figure 3: the configure page of policy route

If want to delete the route rule, select the checkbox button Remove, then click button “Remove”.

Warning：one lan interface can bind with onw wan route PVC, if the lan interface is binded,it will tip add error.

4.4.6.4.5 Test

The test network topology adopted as figure 4：

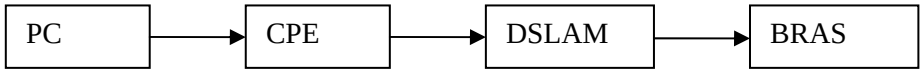


figure4 :the test network topology

Warning：PC should directly connect with CPE by reticle，moreover at the CPE side the reticle should insert into the first interface.

Step1:First config two PPPoE PVC，reset CPE，then two PVC should dial succeed，as figure 5：

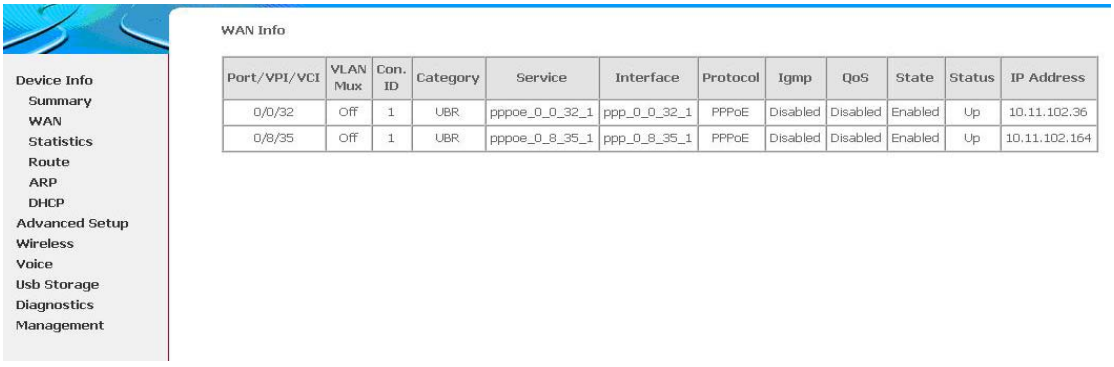


figure 5: two PPPoE PVC dial succeed

Remember two PPPoE PVC obtain IP address, enable port mirror function，the aim is than can catch packet transmit from PVC at the PC.

Step2:In the browser window open http://192.168.1.1/engdebug.cmd，as figure 6:

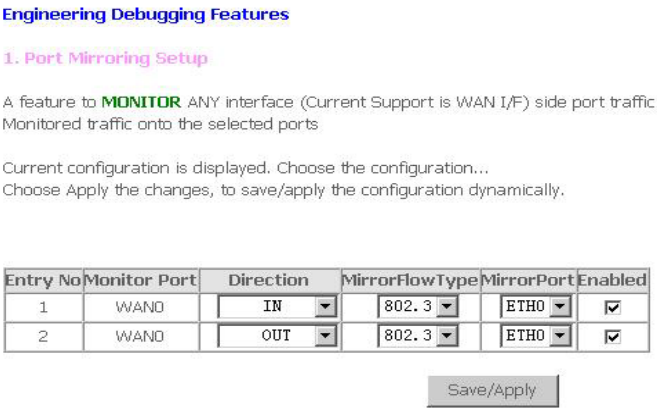


figure 6 :enable port mirror function

step3:Delete all policy route configure, only config ENET1 bind with PVC 0/32, at PC ping the wan side default gateway, in this example it's 10.11.102.2, run catch packet softwar, then we can see the data transmitted from PVC 0/32, as figure 7:

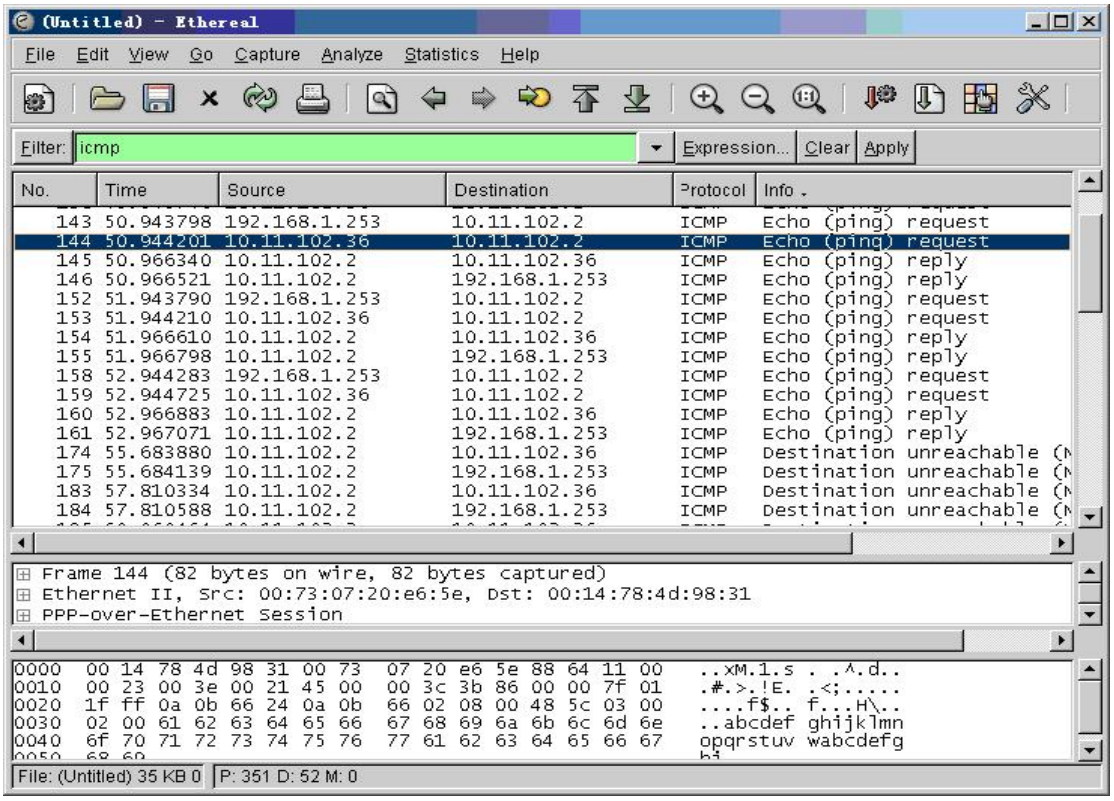


figure 7: the packet transmitted from PVC 0/32

step4:Delete ENT1 bind with PVC 0/32，then bind ENT1 with PVC 8/35，at PC ping wan side default gateway, in this example it's 10.11.102.2，run catch packet softwar, then we can see the data transmitted from PVC 8/35, as figure 8:

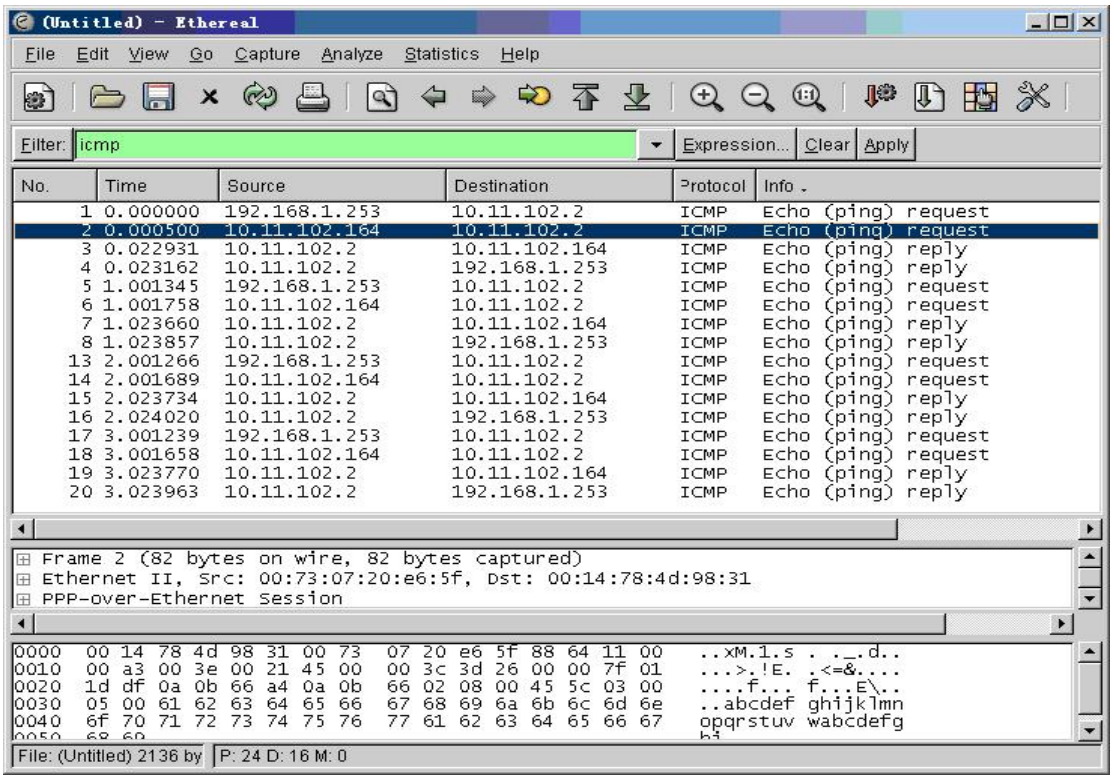


Figure 8 the packet transmitted from PVC 8/35

4.4.7 DNS

Short for **D**omain **N**ame **S**ystem (or **S**ervice or **S**erver), an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4.
The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

4.4.7.1 DNS Server

In this interface, you can modify the DNS server settings.

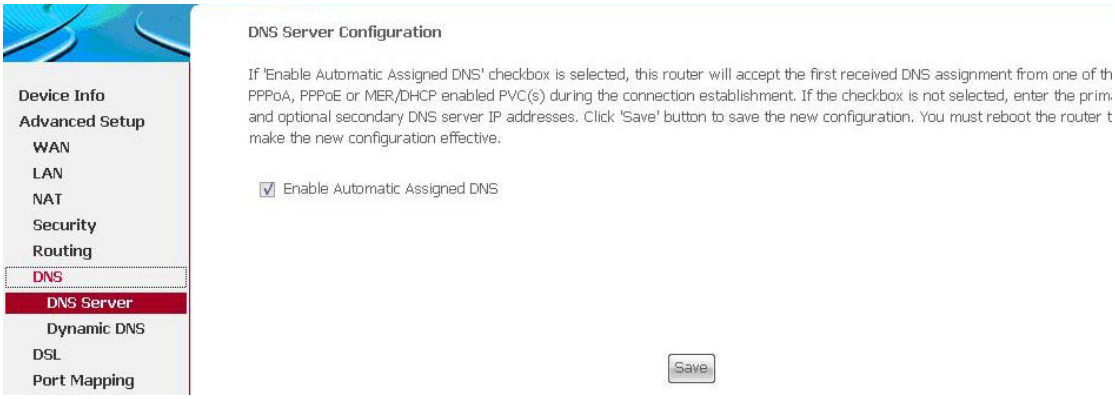

Device Info
Advanced Setup
WAN
LAN
NAT
Security
Routing
DNS
DNS Server
Dynamic DNS
DSL
Port Mapping
DNS Server Configuration
If 'Enable Automatic Assigned DNS' checkbox is selected, this router will accept the first received DNS assignment from one of th
PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the prim
and optional secondary DNS server IP addresses. Click 'Save' button to save the new configuration. You must reboot the router t
make the new configuration effective.
Enable Automatic Assigned DNS
Save

Figure2.8.9.7:DNS Server Configuration overview

If 'Enable Automatic Assigned DNS' checkbox is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the

connection establishment.
If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. The interface is below.

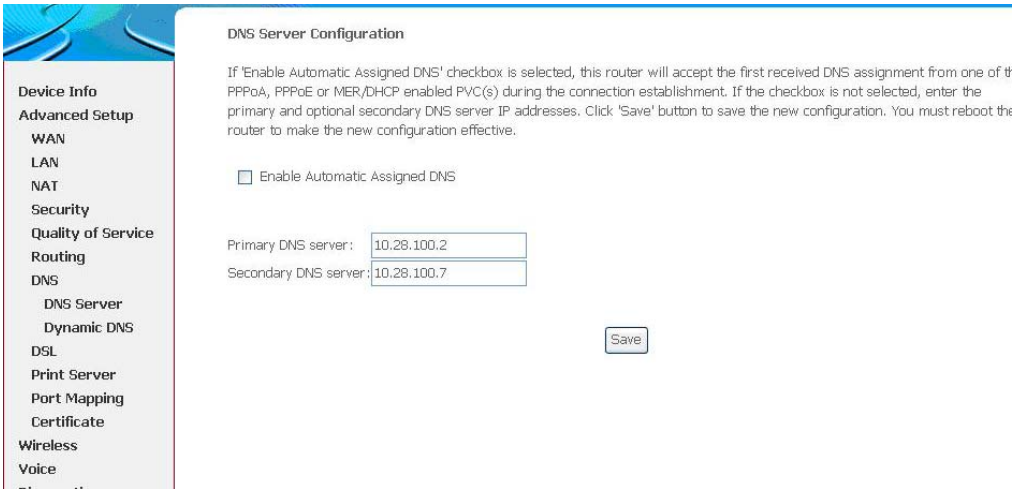

Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Routing
DNS
DNS Server
Dynamic DNS
DSL
Print Server
Port Mapping
Certificate
Wireless
Voice
DNS Server Configuration
If 'Enable Automatic Assigned DNS' checkbox is selected, this router will accept the first received DNS assignment from one of t
PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the
primary and optional secondary DNS server IP addresses. Click 'Save' button to save the new configuration. You must reboot the
router to make the new configuration effective.
Enable Automatic Assigned DNS
Primary DNS server: 10.28.100.2
Secondary DNS server: 10.28.100.7
Save

Figure2.8.9.8: DNS Server Add Configuration

Click 'Save' button to save the new configuration.
NOTE: You must reboot the router to make the new configuration effective.

4.4.7.2 Dynamic DOMAIN NAME SERVICE (DDNS)

4.4.7.2.1 OVERVIEW

Dynamic DNS allows binding of domain names to hosts with dynamically assigned IP addresses by a Dynamic Host Control Protocol (DHCP) server and updates the nameserver with the new information about the host or the network. This is particularly useful to broadband users hosting internet services such as File Transfer Protocol (FTP), Hyper Text Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP) on their local hosts connected to the broadband network at home. Dynamic DNS allows access to such hosts connected to the broadband networks using a domain name to exchange files, send receive email with highly personalized email addresses and host a website. The primary requirement in such case is for the domain name to be associated with the ever changing IP address of the host or the network. For more details about dynamic DNS please refer to RFC 2136.

To provide such support for the feature described above, a client is installed in the host serving the internet traffic directed to the domain. The client updates the IP address of the host whenever the host renegotiates the IP address for any reason. The BCM963xx Linux reference software provides support for dynamic DNS allows the users to configure the following dynamic DNS servers for DDNS service:

- **DynDNS.org**: A free DNS service for hosts with dynamic IP addresses.
- **TZO**: A service provider providing dynamic and static DNS services for a fee.

To use one of the providers mentioned above requires the users to register with the dynamic DNS service provider the information about the host and the install the client software on the host which can update the service provider with the IP address and the domain name information.

4.4.7.2.2 CONFIGURATION

The DDNS feature in Linux reference software requires to be configured in the menuconfig to include the support for this feature. Once the software support is configured to be built for a profile, this feature can be configured using the WEB UI as:

- Choose the Advanced Setup from the WEB UI, choose the DNS menu item under Advanced Setup and select the Dynamic DNS menu item under DNS.

Figure2.8.9.9: Dynamic DNS Configuration overview

- Click the Add button to configure a new host information.

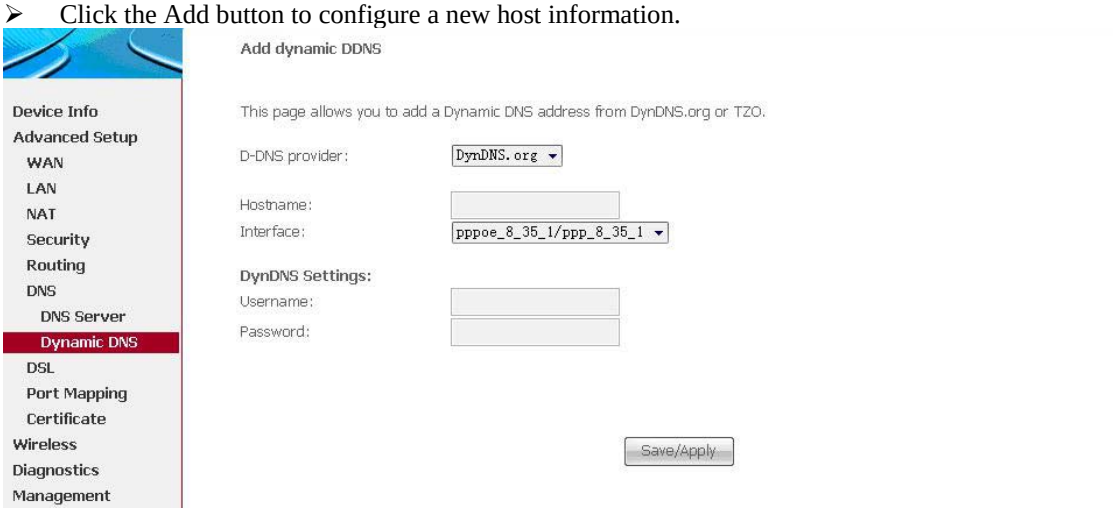


Figure2.8.9.10: Dynamic DNS Add Configuration

D-DNS provider: Dynamic DNS provider's website.
Hostname: This is the domain name which can be modified.
Interface: The interface that the packets pass through on the MODEM.
Username: This is the Username needed access the DDNS's management interface.
Password: This is the Password you will be prompted to enter when you access the DDNS's management interface.

- Select the service provider for the DDNS service, provide the hostname and the interface to use when sending the DDNS updates. Also enter the service provider specific registration information and click Save/Apply to use the feature.

4.4.8 DSL

In this interface, you can check the DSL settings. Mostly, the user just need to remain this factory default setting. Our modem support these modulations: G.Dmt, G.lite, T1.413, ADSL2, AnnexL, ADSL2+ and AnnexM. The MODEM will negotiate the modulation mode with the DSLAM.

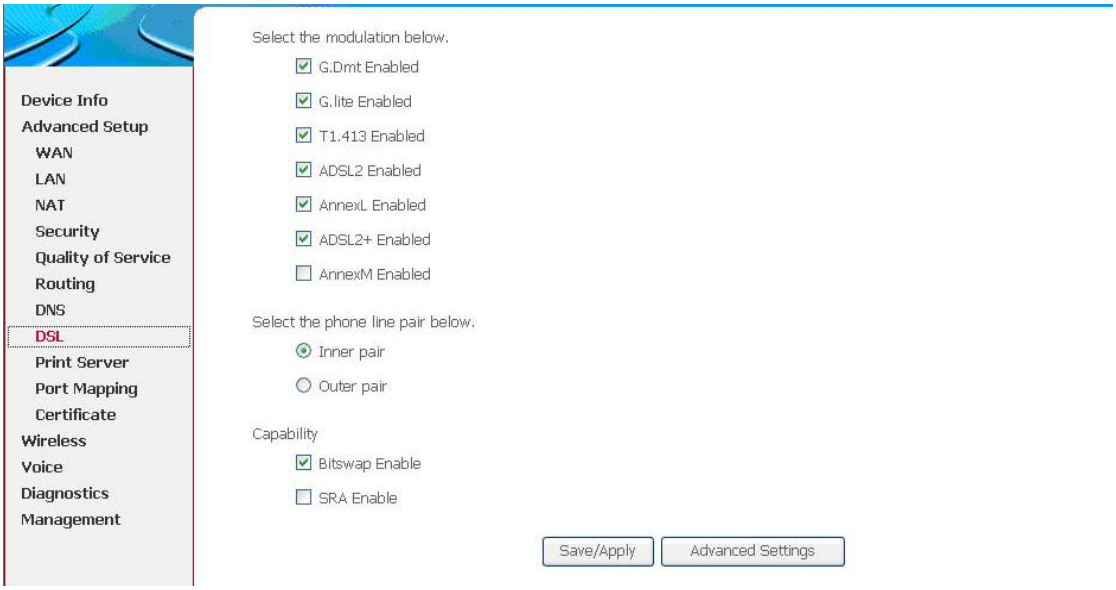


Figure2.9.1 :DSL modulation settings

4.4.9 Print Server

A network printer is a printer on which you can print your documents without it being connected to your pc. The advantage of this is that you only need this printer once in your network. All PCs for which it is released can access it and work with it.
In most cases a printer of this type is connected to another PC in the network. This does indeed offer the advantage referred to above, but it has serious disadvantages:

- The printer can only be used by others if the PC to which it is connected is switched on.
- The print job you send to the PC on which the printer depends reduces the performance of this PC.

To facilitate this option you must first set up a printer port on each PC that is to use the network printer. A printer port is an interface on the PC that forwards the print job to an IP address within the network. Once you have set up this port you must install the printer driver.

4.4.9.1 Configuring Print Server on DSL Server

Following are the steps to enable the on-board Printer Server.
Step1: Enable Print Server from Modem Web GUI.
Step2: Check “Enable on-board printer server” and key in “Printer name”, “Make and model”.
Note:
The “Printer name” can be any text string up to 40 characters.
The “Make and model” can be any text string up to 128 characters.

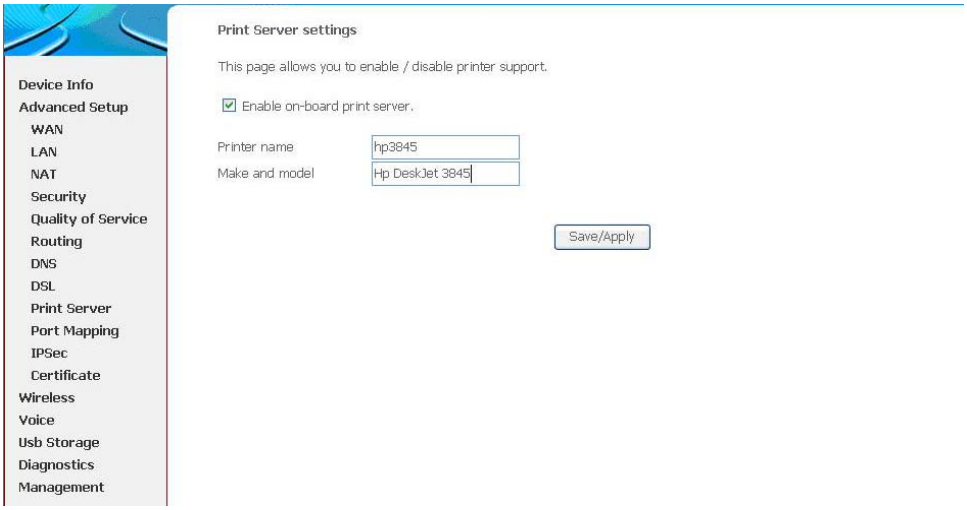
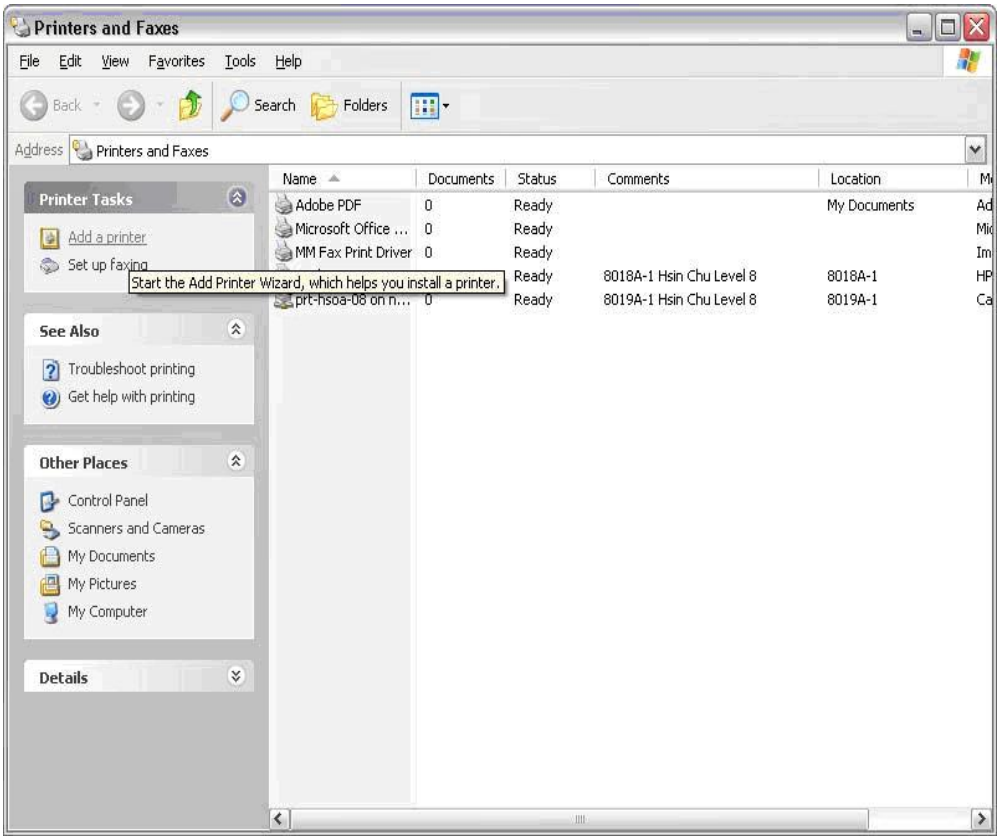


Figure2.9.2: Print Server Config

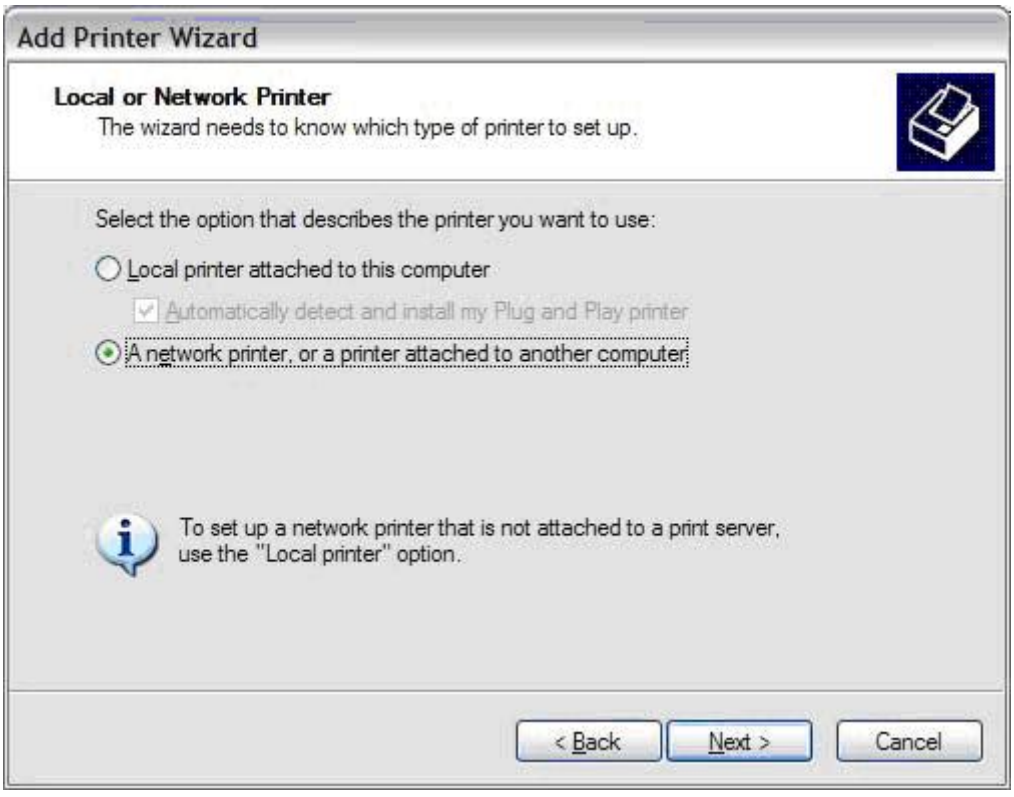
4.4.9.2 Configuring Print Server on the Windows Host

The configuring sequence:
Step1: Click on Add a printer from **Control Panel** of the **Win XP** computer and click “Next”.



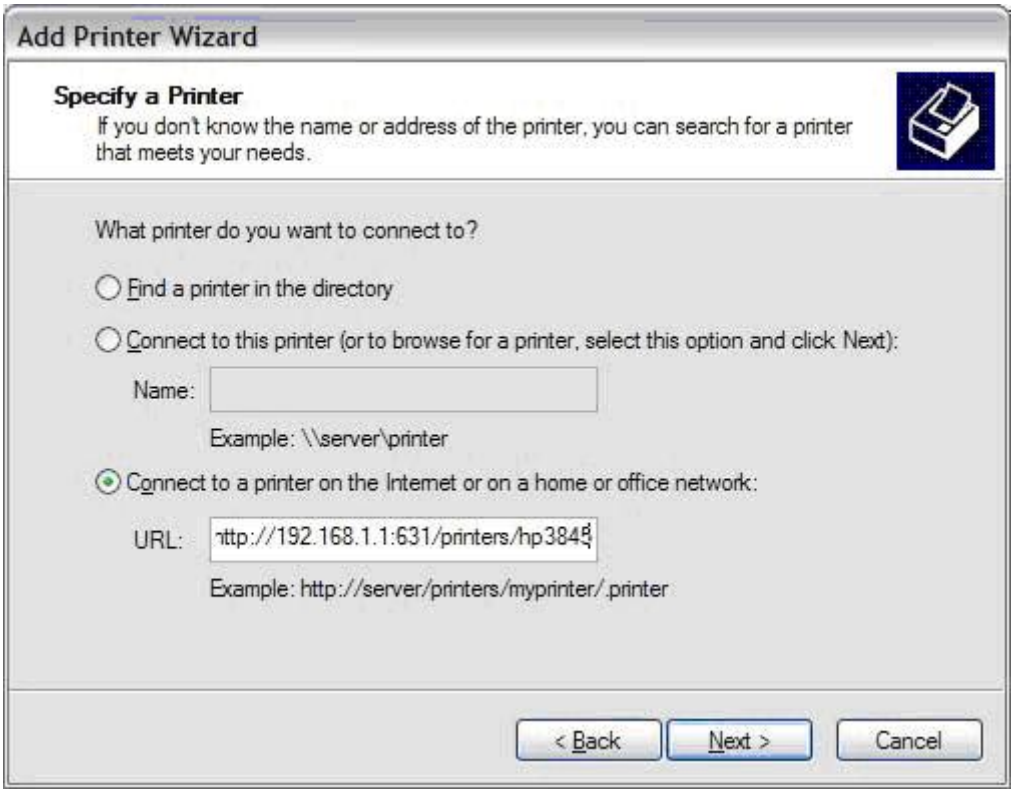
Add Printer Wizard
Welcome to the Add Printer Wizard
This wizard helps you install a printer or make printer connections.
If you have a Plug and Play printer that connects through a USB port (or any other hot pluggable port, such as IEEE 1394, infrared, and so on), you do not need to use this wizard. Click Cancel to close the wizard, and then plug the printer's cable into your computer or point the printer toward your computer's infrared port, and turn the printer on. Windows will automatically install the printer for you.
To continue, click Next.
< Back
Next >
Cancel

Step2: Select Network Printer and click "Next".


Add Printer Wizard
Local or Network Printer
The wizard needs to know which type of printer to set up.
Select the option that describes the printer you want to use:
Local printer attached to this computer
Automatically detect and install my Plug and Play printer
A network printer, or a printer attached to another computer
To set up a network printer that is not attached to a print server, use the "Local printer" option.
< Back
Next >
Cancel

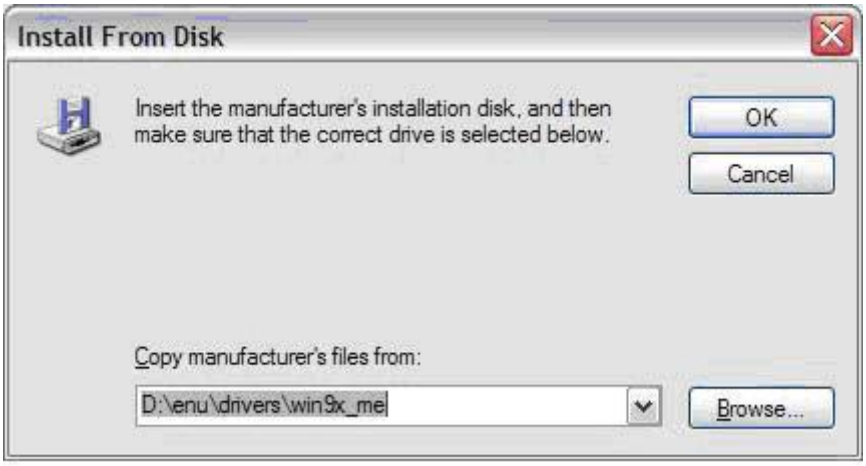
Step3: Select Connect to a printer on the Internet, type "http://192.168.1.1:631/printers/hp3845" and click "Next".

The printer name "hp3845" must be the same name entered in the ADSL modem WEB UI "printer server setting" as in step 1.


Add Printer Wizard
Specify a Printer
If you don't know the name or address of the printer, you can search for a printer that meets your needs.
What printer do you want to connect to?
Find a printer in the directory
Connect to this printer (or to browse for a printer, select this option and click Next):
Name:
Example: \\server\printer
Connect to a printer on the Internet or on a home or office network:
URL:
http://192.168.1.1:631/printers/hp384
Example: http://server/printers/myprinter/.printer
< Back
Next >
Cancel

Step 4: Click “Have Disk”, insert printer driver CD.

Step 5: Select driver file directory on CD-ROM and click “OK”.



4.4.10 Port Mapping

Port Mapping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.
Selecting the “Enable virtual ports” button in WEB UI “Port Mapping” page will create three virtual interfaces within the Linux system. Each virtual interface represents a physical Ethernet port within the external Ethernet Switch. The WEB UI will display four Ethernet ports: ENET1, ENET2, ENET3, and ENET4. ENET1, ENET2, and ENET3 represent Ethernet port ID 0, 1 and 2 within the Ethernet Switch. ENET4 represents the Ethernet MAC/PHY MDI port.
De-selecting the “Enable virtual ports” button will disable the system capability to recognize individual Ethernet port within the Ethernet switch. The WEB UI will display two Ethernet ports, ENET(1-3) and ENET4. The ENET(1-3) represents the Ethernet MAC MII port. The ENET4 represents the BCM634x Ethernet MAC/PHY MDI port.

4.4.10.1 Create a new mapping group

Group Name: Enter a unique group name.
Grouped Interfaces: The port belongs to this group.
Available Interfaces: It shows the available Ethernet port which you can select.
Automatically Add Clients With the following DHCP Vendor IDs: If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address. (for example, the windows 2000/XP default DHCP client’s vender ID is MSFT 5.0.).

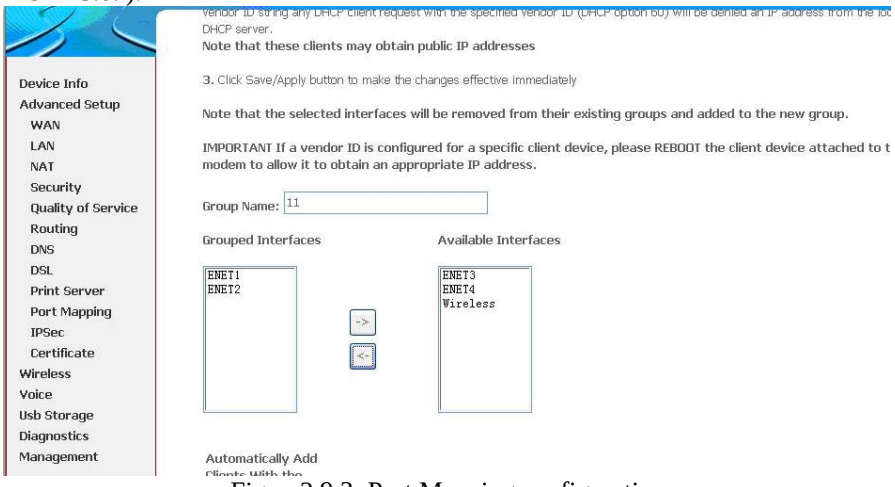
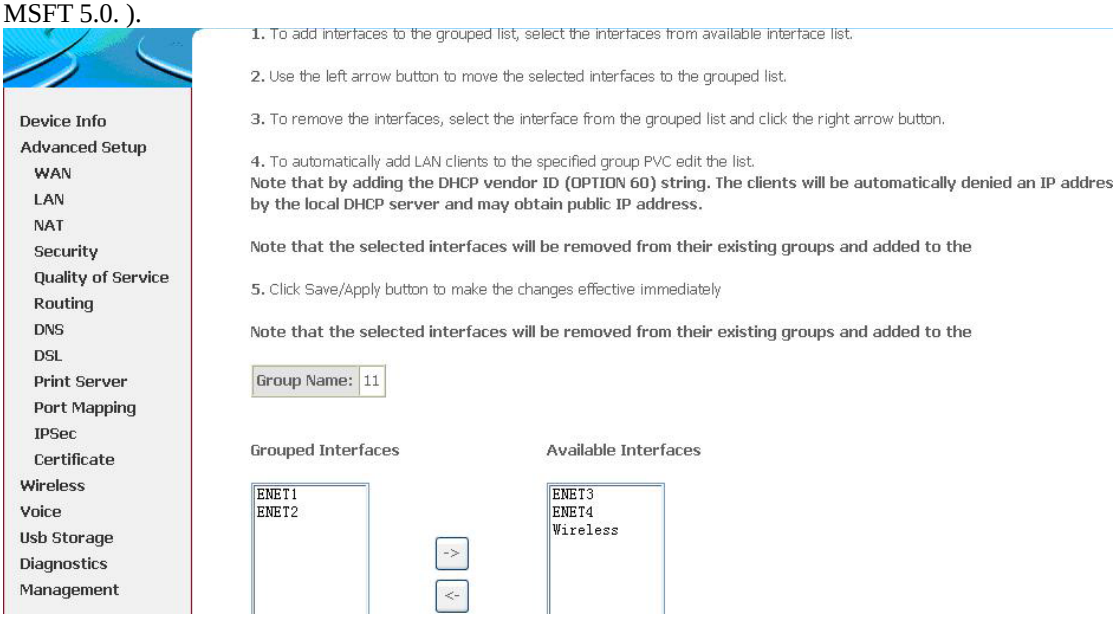


Figure2.9.3: Port Mapping configuration

Step1: Enter the Group name and select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. The group name must be unique.
Step2: If you like to automatically add LAN clients to a PVC in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.
Note that these clients may obtain public IP addresses
Step3: Click Save/Apply button to make the changes effective immediately
Note: That the selected interfaces will be removed from their existing groups and added to the new group.

4.4.10.2 Edit a existing group

Group Name: Enter a unique group name.
Grouped Interfaces: The port belongs to this group.
Available Interfaces: It shows the available Ethernet port which you can select.
Automatically Add Clients With the following DHCP Vendor IDs: If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address. (for example, the windows 2000/XP default DHCP client's vender ID is MSFT 5.0.).


Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Routing
DNS
DSL
Print Server
Port Mapping
IPSec
Certificate
Wireless
Voice
Usb Storage
Diagnostics
Management
1. To add interfaces to the grouped list, select the interfaces from available interface list.
2. Use the left arrow button to move the selected interfaces to the grouped list.
3. To remove the interfaces, select the interface from the grouped list and click the right arrow button.
4. To automatically add LAN clients to the specified group PVC edit the list.
Note that by adding the DHCP vendor ID (OPTION 60) string. The clients will be automatically denied an IP addres by the local DHCP server and may obtain public IP address.
Note that the selected interfaces will be removed from their existing groups and added to the
5. Click Save/Apply button to make the changes effective immediately
Note that the selected interfaces will be removed from their existing groups and added to the
Group Name: 11
Grouped Interfaces
Available Interfaces
ENET1
ENET2
->
<-
ENET3
ENET4
Wireless
Figure2.9.4: Edit Port Mapping Configuration

Edit Port Mapping Configuration
Step1: To add interfaces to the grouped list, select the interfaces from available interface list.
Step2: Use the left arrow button to move the selected interfaces to the grouped list.
Step3: To remove the interfaces, select the interface from the grouped list and click the right arrow button.
Step4: To automatically add LAN clients to the specified group PVC edit the list.
Note: That by adding the DHCP vendor ID (OPTION 60) string. The clients will be automatically denied an IP address by the local DHCP server and may obtain public IP address.
Note: That the selected interfaces will be removed from their existing groups and added to the
5. Click Save/Apply button to make the changes effective immediately
Note: That the selected interfaces will be removed from their existing groups and added to the

4.4.11 IPsec

IPSec (Internet Protocol Security Associations) allows creation of secure tunnels in the IP (Internet Protocol) layer. Secure tunnels are used to construct VPNs (Virtual Private Networks) over the internet. The IPSec protocol design includes ISAKMP (Internet Security Association Key Management Protocol)

framework and IKE (Internet Key Exchange) protocol is the primary protocol to generate and maintain IPSec SAs (Security Associations), which are the basic building blocks of VPNs (Virtual Private Networks) over the internet. IKE uses cryptography extensively. However, for our purpose we will assume that cryptography is a module to generate a key and use it to encrypt or decrypt the payload. Once the SAs are established the payload is transferred using IPSec ESP (Encapsulating Security Payload) or AH (Authentication Header) protocols. Of the two payload transfer protocols ESP and AH, the former is most widely used and suitable for NAT operation.
IPsec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion (*payload*) of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPSec-compliant device decrypts each packet.
For IPsec to work, the sending and receiving devices must share a public key. This is accomplished through a protocol known as *Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley),* which allows the receiver to obtain a public key and authenticate the sender using digital certificates.

4.4.11.1 VPNs (Virtual Private Networks)

A virtual private network (VPN) provides a secure connection between a sender and a receiver over a public non-secure network such as the Internet. A secure connection is generally associated with private networks. (A private network is a network that is owned, or at least controlled via leased lines, by an organization.) Using the techniques discussed later in this chapter, a VPN can transform the characteristics of a public non-secure network into those of a private secure network. VPNs reduce remote access costs by using public network resources. Compared to other solutions, including private networks, a VPN is inexpensive.
VPNs are not new. In fact, they have been used in telephone networks for years and have become more prevalent since the development of the intelligent network. Frame relay networks, which have been around for some time, are VPNs. Virtual private networks are only new to IP networks
such as the Internet. Therefore, some authors use the terms *Internet VPN* and *virtual private data network* to distinguish the VPN described in this chapter from other VPNs. In this book, the term VPN refers to Internet VPN.
The goal of a VPN is to provide a secure passage for users' data over the non-secure Internet. It enables companies to use the Internet as the virtual backbone for their corporate networks by allowing them to create secure *virtual* links between their corporate office and branch or remote offices via the Internet. The cost benefits of VPN service have prompted corporations to move more of their data from private WANs to Internet-based VPNs.

4.4.11.2 ISAKMP

ISAKMP, Short for Internet Security Association Key Management Protocol, is a definition of a high level abstract framework for point to point, two party asymmetric key management protocols. Being asymmetric one party assumes the role of ***initiator***, which begins the exchange of protocol messages by sending the first message. The second is the ***responder*** which replies to the first message from the ***initiator***. ISAKMP makes a distinction between a key exchange and key management (when the key is rolled to the next one). Key exchange is mainly concerned with exchanging information to generate secret keys shared between two parties. ISAKMP negotiation is divided into two phases. In the first phase ISAKMP SA (Security Association) is established between two entities to protect further negotiation traffic. The second phase SA is used for some security protocol. The key exchange protocol must:

- Generate a set of secret keys shared between the intiator and the responder.
- Authenticate the identity of the initiator and the responder.
- Ensure independence of the sets of keys generated. This property is also known as PFS (Perfect Forward Secrecy).
- Key exchange protocol must be scalable.

Once the keys are generated and shared there must be some meta parameters agreed between the parties to use the keys. The following are the meta parameters to use the keys:

- Cryptographic algorithms and parameters to the cryptographic algorithms to be used with the keys.
- How to apply the cryptographic algorithms and keys.

- Key lifetime and refreshment policy.

4.4.11.3 IKE (Internet Key Exchange)

The Internet Key Exchange (IKE) protocol is a key management protocol standard which is used in conjunction with the IPSec standard. IPSec is an IP security feature that provides robust authentication and encryption of IP packets.
IPSec can be configured without IKE, but IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard.
IKE is a hybrid protocol which implements the **OAKLEY** key exchange and **SKEME** key exchange inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. (ISAKMP, OAKLEY, and SKEME are security protocols implemented by IKE.)

- **OAKLEY:** Describes a specific mechanism for exchanging keys through the definition of various key exchange "modes". Most of the IKE key exchange process is based on OAKLEY.

- **SKEME:** Describes a different key exchange mechanism than OAKLEY. IKE uses some features from SKEME, including its method of public key encryption and its fast re-keying feature.

4.4.11.4 How to use and configure the IPSec

To use IPSec user interface, choose "IPSec" under "Advanced Setup" menu. The base screen will be shown:

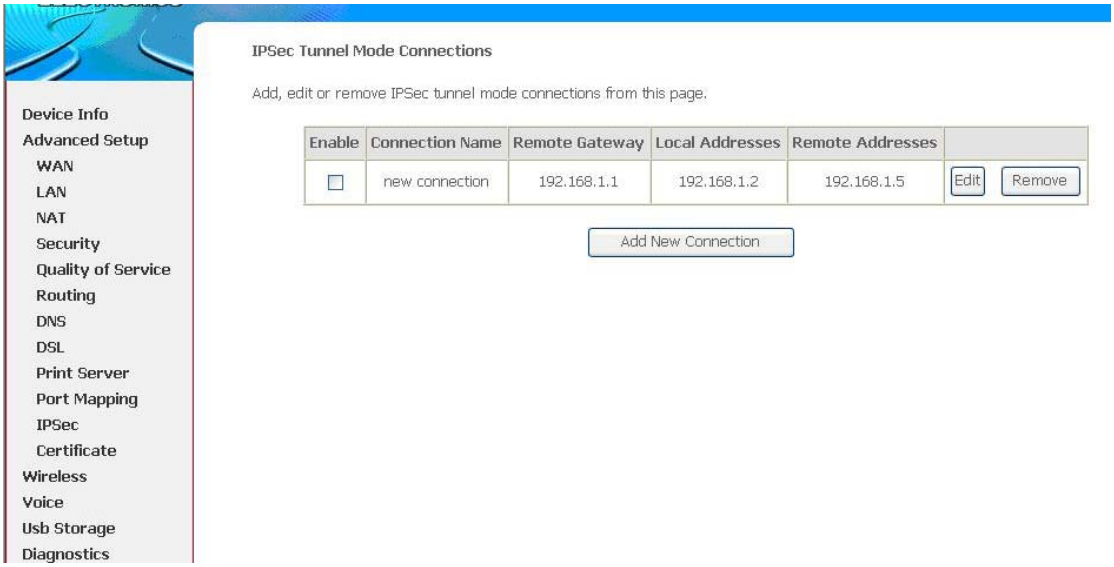


Figure2.9.5:IPSec Tunnel Mode Connections

The table shows current connections. User can control the following items in the base IPSec page:
• Click the check box under "Enable" column to enable or disable the connection.
• Click the "Remove" button to remove a connection
• Click the "Add New Connection" button to add a new connection
• Click the "Edit" button to edit a existing connection

4.4.11.4.1 IPSec Setting Parameters

- **IPSec Connection Name:** Enter a name for the new connection.
- **Remote IPSec Gateway Address:** the remote modem (which you want to connection) IP Gateway of WAN side
- **Tunnel access from local IP addresses:** if you select "single Address" it allow only one PC from local to connect remote hosts with IPSEC mode. And you must input the PC's IP address in

4th. item

If you select “subnet ” it allow more than one PC from local to connect remote hosts with IPSEC mode. Notice: these PCs must in the same subnet ,you must input the subnet address in 4th item. And input the subnet mask in the “IP Subnet mask” which will hide when you choose “single Address”.

- **IP Address for VPN:** the PC’s IP address (if you select “single Address”)/the subnet address (if you choose “subnet”)
- **Tunnel access from remote IP addresses:** same with the third item, but it means remote modem.
- **Key Exchange for VPN:** You can select the encrypt mode, (Auto(IKE), and manual), The “Auto (IKE) will set the encrypt auto, the other need you set the encrypt manual.

4.4.11.4.2 The example to configure IPSec

The following screen is used to edit configurations when adding or editing an IPSec connection:

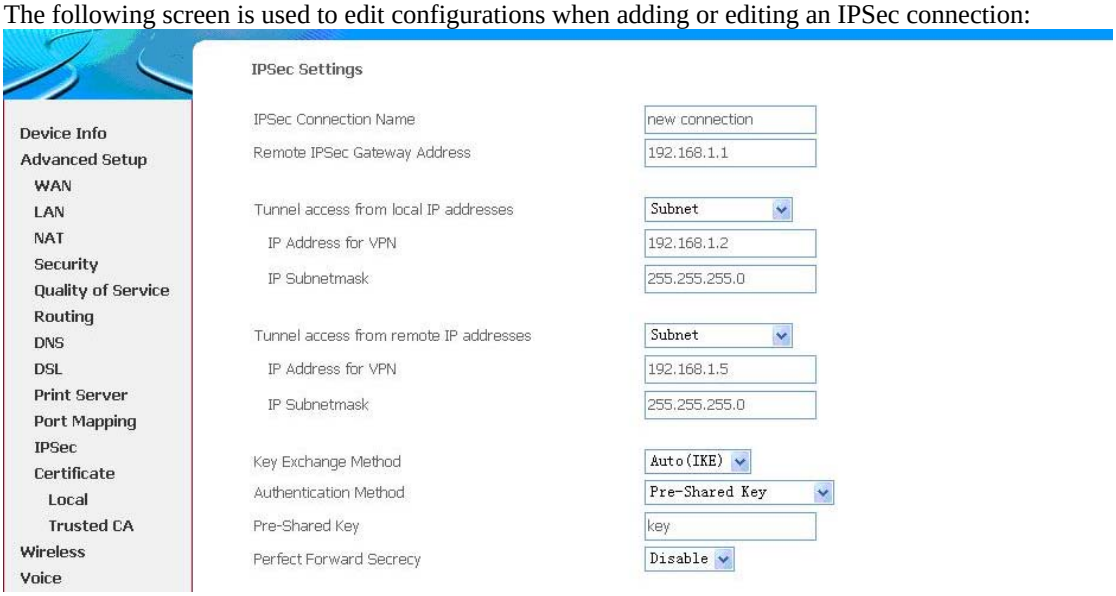


Figure2.9.6:IPSec Configure example

This is a dynamic page. It will change itself by showing and hiding options when different types or connections are chosen. User can select automatic key exchange or manual key exchange, pre-shared key authentication or certificate authentication, etc.

When automatic key exchange method is used, click “Show Advanced Settings” will show more options:

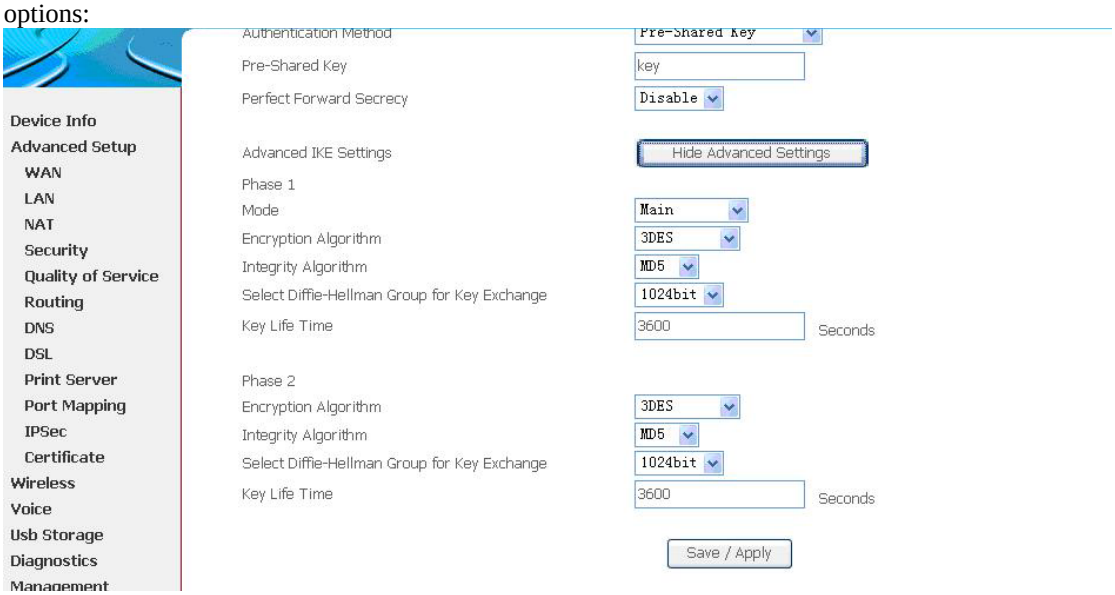


Figure2.9.7: automatic key exchange advanced settings

4.4.12 Certificate

To use Certificate user interface, choose “Certificate” under “Advanced Setup” menu. There are two menu items under “Certificate” menu: “Local” and “CA”. For either type of certificate, the base screen shows a list of certificates stored in modem.

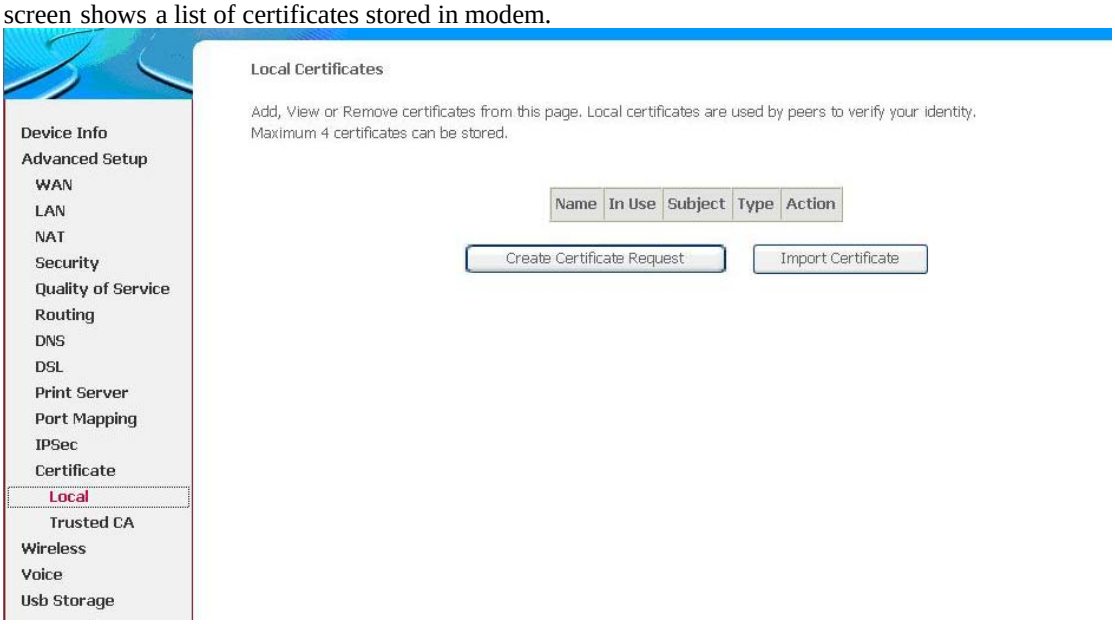


Figure2.9.8: Local Certificate overview

In the menu, “Local” means local certificates. “Trusted CA” means trusted Certificate Authority certificates. Local certificates preserve the identity of the modem. CA certificates are used by the modem to very certificates from other hosts.
Local certificates can be created by two ways:

- Create a new certificate request, have it signed by a certificate authority and load the signed certificate
- Import an existing signed certificate directly

4.4.12.1 Create New Local Certificate

Certificate name: Creates an SSL certificate in the specified certificate repository (administrator's or domain's repository) by using a private key file and a corresponding certificate file.

Common Name: The common name is the "fully qualified domain name," (or FQDN) used for DNS lookups of your server (for example, www.mydomain.com). Browsers use this information to identify your Web site. Some browsers will refuse to establish a secure connection with your site if the server name does not match the common name in the certificate. Please do not include the protocol specifier "http://" or any port numbers or pathnames in the common name. Do not use wildcard characters such as * or ?, and do not use an IP address.

Organization Name: The name of the organization to which the entity belongs (such as the name of a company).

State/Province Name: This is the name of the state or province where your organization's head office is located. Please enter the full name of the state or province.

Country/Region Name: This is the two-letter ISO abbreviation for your country (for example, GB for the United Kingdom).

Follow the following steps to create a new certificate:
Click “Create Certificate Request”, enter necessary information:

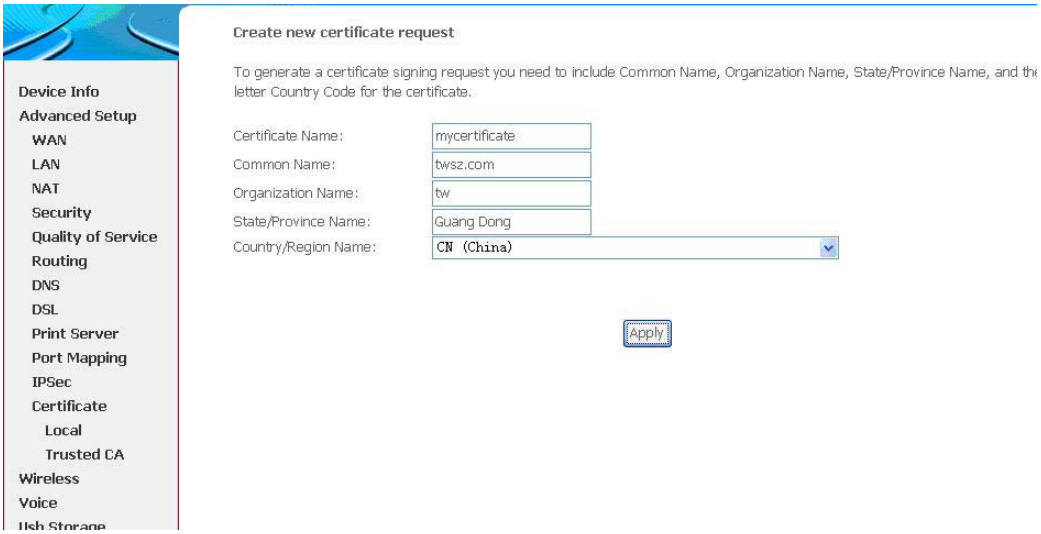


Figure2.9.9: create new certificate request

Wait several seconds, the generated certificate request will be shown:

Figure3.1.1: generated certificate request

The certificate request needs to be submitted to a certificate authority, which would sign the request. Then the signed certificate needs to be loaded into modem. Click “Load Certificate” button from the previous screen or from the base screen will bring up the load certificate page. Paste the signed certificate and click apply and a new certificate is created.

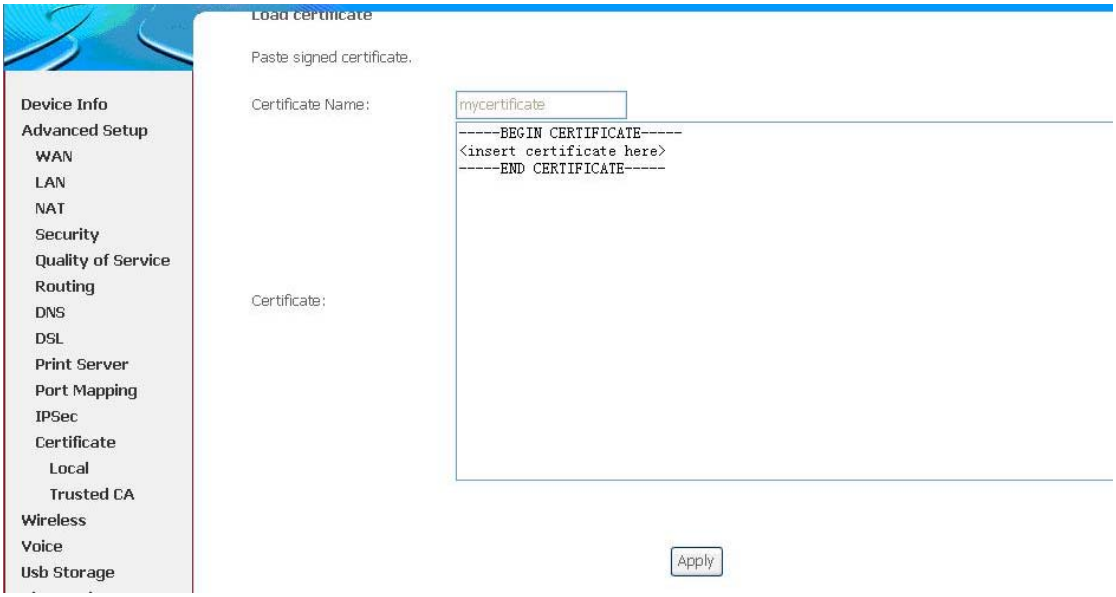


Figure3.1.2: Load Certificate

4.4.12.2 Import Existing Local Certificate

To import existing certificate, click “Import Certificate” button and paste both certificate and corresponding private key:

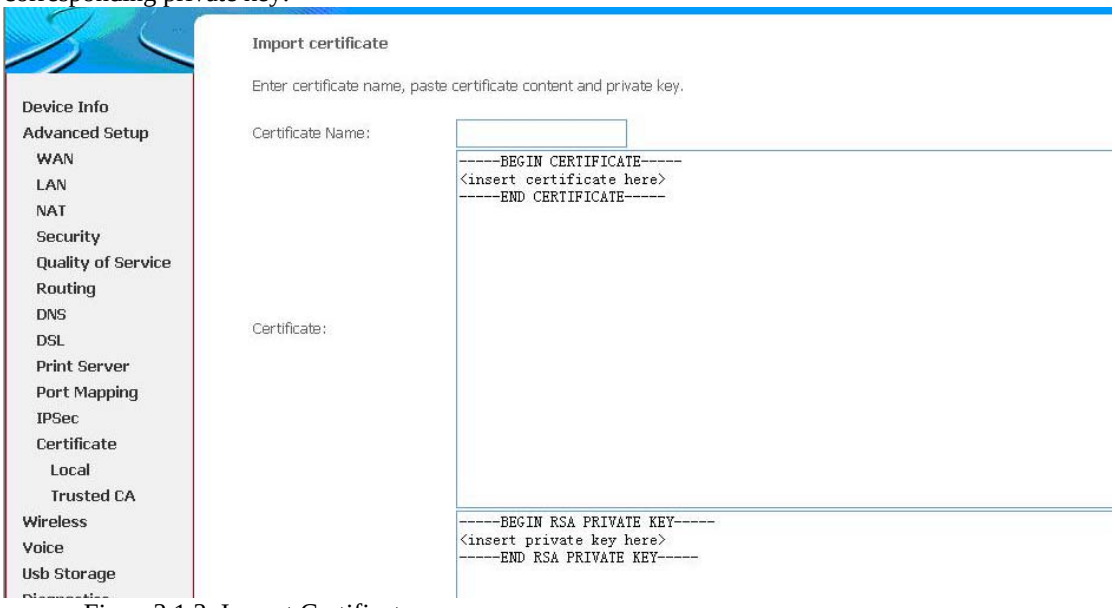


Figure3.1.3: Import Certificate

4.4.12.3 Trusted CA Certificates

Click “Certificate” --> “Trusted CA” to show the interface. CA certificates are used by you to verify peers' certificates. Maximum 4 certificates can be stored.

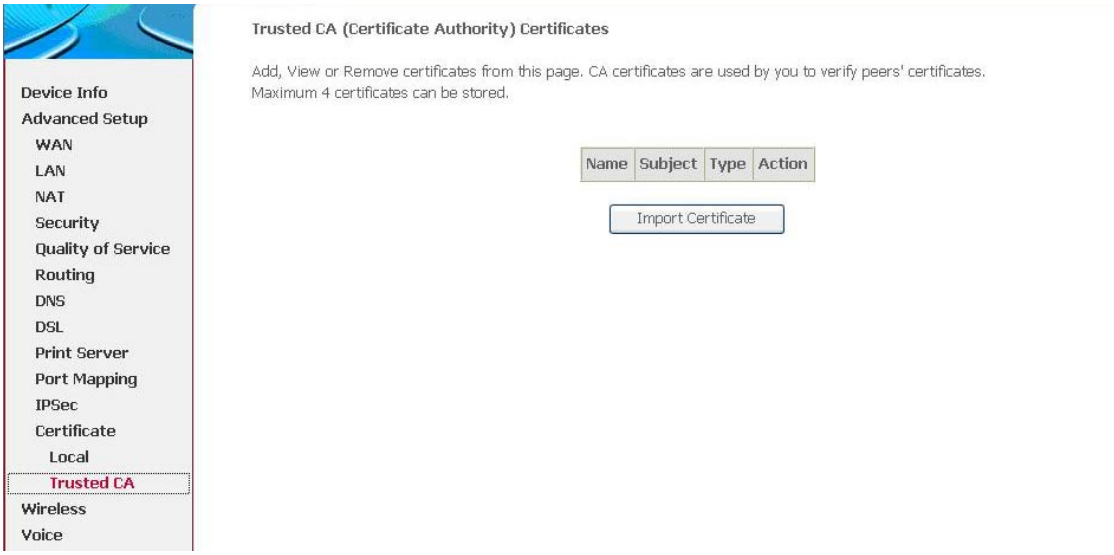


Figure3.1.4: Trusted CA certificates

Click “Import Certificate”. CA certificate can only be imported. The screen for importing is shown below:

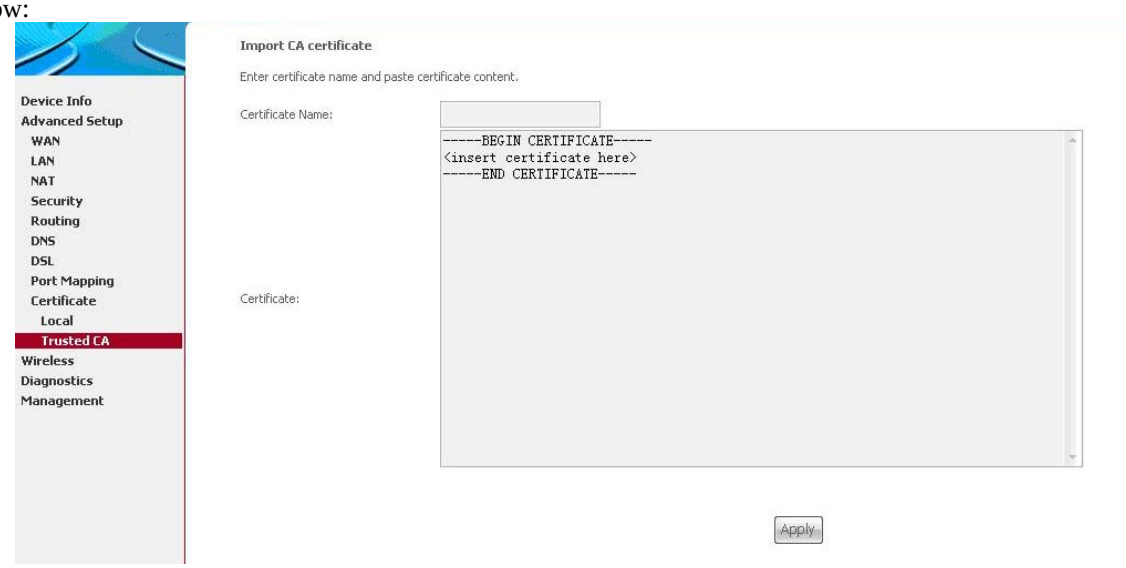


Figure3.1.5: Import CA Certificate

4.5 Wireless

4.5.1 Overview

4.5.1.1 What is wireless network

There are two types of wireless network set ups: Client Mode (infrastructure) and Ad Hoc Mode (peer-to-peer). Client Mode is an 802.11 networking framework in which devices communicates with each other by first going through a wireless router or access point. Wireless devices can communicate with each other or can communicate with a wired network. Generally, a majority of small businesses and home users operate in Client Mode because they require access to the wired LAN (usually from broadband or cable Internet providers) in order to use services such as file servers or printers.

Figure 1 Client Model

Ad Hoc (sometimes referred to as peer-to-peer), is a type of wireless network allowing a wireless adapter or other Ethernet-ready device to connect directly to another wireless adapter or Ethernet-ready device.

Figure 2 Ad Hoc Model

4.5.1.2 About our product

The Gawv5.4U4-A3 Wi-Fi® certified IEEE 802.11g compliant wireless access point allows multiple computers to connect wirelessly to your local network over the Gawv5.4U4-A3 Wireless LAN environment. The Gawv5.4U4-A3 is backward compatible with IEEE 802.11b, which means 802.11b and 802.11g devices can coexist in the same wireless network. The Wireless Distribution System (WDS) on your Gawv5.4U4-A3 allows you to extend the range of your wireless network. To be able to use WDS, you will need to introduce an additional WDS-enabled access point into your wireless network. To be able to connect the computers, make sure that a wireless client adapter (WLAN client) is installed on each computer you want to connect via the WLAN.

4.5.2 Wireless LAN Basics

Some basic understanding of 802.11b/g wireless technology and terminology is useful when you are setting up the Router or any wireless access point. If you are not familiar with wireless networks please take a few minutes to learn the basics.

4.5.2.1 Basic terms

Before introducing the terms, Let’us see a typical wireless network topology.

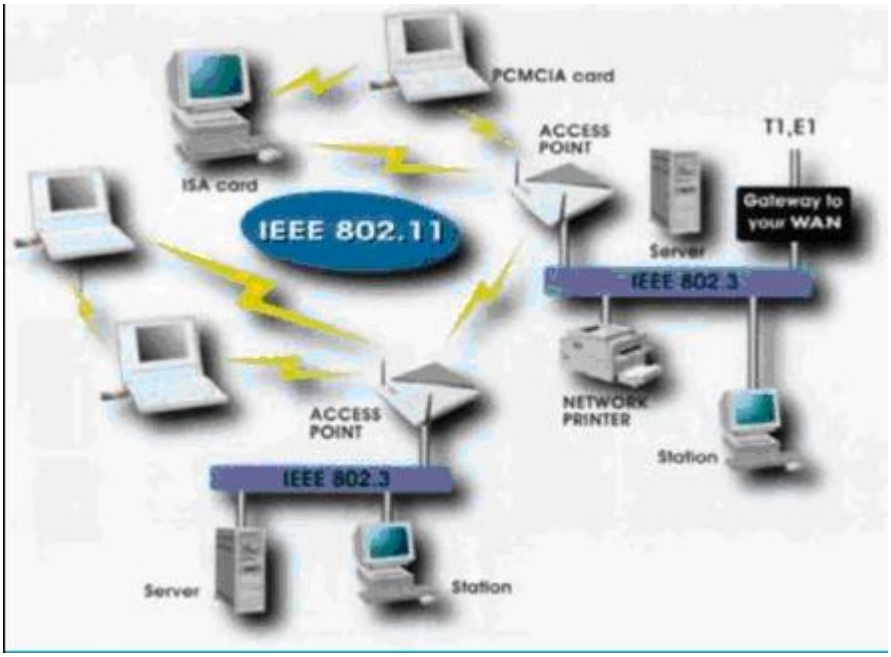


Figure3： A typical wireless network topology

In the graphic, few terms should be understood.

·AP: Short for ***A**ccess **P**oint*, a hardware device or a computer's software that acts as a communication hub for users of a wireless device to connect to a wired LAN. APs are important for providing heightened wireless security and for extending the physical range of service a wireless user has access to.

·STA: Any device that contains an IEEE 802.11 conformant medium access control (MAC) and physical layer (PHY) interface to the wireless medium (WM).

·SSID: Wireless networks use an SSID (Service Set Identifier) to allow wireless devices to roam within the range of the network. Wireless devices that wish to communicate with each other must use the same SSID. Several access points can be set up using the same SSID so that wireless stations can move from one location to another without losing connection to the wireless network. The Gawv5.4U4-A3 operates in Infrastructure mode. It controls network access on the wireless interface in its broadcast area. It will allow access to the wireless network to devices using the correct SSID after a negotiation process takes place. By default the Gawv5.4U4-A3 broadcasts its SSID so that any wireless station in range can learn the SSID and ask permission to associate with it. Many wireless adapters are able to survey or scan the wireless environment for access points. An access point in Infrastructure mode allows wireless devices to survey that network and select an access point with which to associate. You may disable SSID broadcasting in the web manager’s wireless menu.

4.5.2.2 Wireless Standard

Wireless Standard include **802.11a**, **802.11b**, **802.11g**, and **802.11n.**

802.11b IEEE expanded on the original 802.11 standard in July 1999, creating the *802.11b* specification. 802.11b supports bandwidth up to 11 Mbps, comparable to traditional Ethernet. 802.11b

uses the same *unregulated* radio signaling frequency (2.4 GHz) as the original 802.11 standard. Vendors often prefer using these frequencies to lower their production costs. Being unregulated, 802.11b gear can incur interference from microwave ovens, cordless phones, and other appliances using the same 2.4 GHz range. However, by installing 802.11b gear a reasonable distance from other appliances, interference can easily be avoided.

In 2002 and 2003, WLAN products supporting a newer standard called *802.11g* emerged on the market. 802.11g attempts to combine the best of both 802.11a and 802.11b. 802.11g supports bandwidth up to 54 Mbps, and it uses the 2.4 Ghz frequency for greater range. 802.11g is backwards compatible with 802.11b, meaning that 802.11g access points will work with 802.11b wireless network adapters and vice versa.

While 802.11b was in development, IEEE created a second extension to the original 802.11 standard called *802.11a*. Because 802.11b gained in popularity much faster than did 802.11a, some folks believe that 802.11a was created after 802.11b. In fact, 802.11a was created at the same time. Due to its higher cost, 802.11a is usually found on business networks whereas 802.11b better serves the home market.

802.11a supports bandwidth up to 54 Mbps and signals in a regulated frequency spectrum around 5 GHz. This higher frequency compared to 802.11b shortens the range of 802.11a networks. The higher frequency also means 802.11a signals have more difficulty penetrating walls and other obstructions.

Because 802.11a and 802.11b utilize different frequencies, the two technologies are incompatible with each other. Some vendors offer hybrid **802.11a/b** network gear, but these products merely implement the two standards side by side (each connected devices must use one or the other).

Use this chart below to get some quick information to help you differentiate between the available wireless networking standards

Standard	Data Rate	Modulation Scheme	Security	Pros/Cons & More Info
IEEE802.11	Up to 2Mbps in the 2.4GHz band	FHSS or DSSS	WEP & WPA	This specification has been extended into 802.11b.
IEEE 802.11a (Wi-Fi)	Up to 54Mbps in the 5GHz band	OFDM	WEP & WPA	Products that adhere to this standard are considered "Wi-Fi Certified." Eight available channels. Less potential for RF interference than 802.11b and 802.11g. Better than 802.11b at supporting multimedia voice, video and large-image applications in densely populated user environments. Relatively shorter range than 802.11b. Not interoperable with 802.11b.
IEEE 802.11b (Wi-Fi)	Up to 11Mbps in the 2.4GHz band	DSSS with CCK	WEP & WPA	Products that adhere to this standard are considered "Wi-Fi Certified." Not interoperable with 802.11a. Requires fewer access points than 802.11a for coverage of large areas. Offers high-speed access to data at up to 300 feet from base station. 14 channels available in the 2.4GHz band (only 11 of which can be used in the U.S. due to FCC regulations) with only three non-overlapping channels.
IEEE 802.11g (Wi-Fi)	Up to 54Mbps in the 2.4GHz band	OFDM above 20Mbps, DSSS with CCK below 20Mbps	WEP & WPA	Products that adhere to this standard are considered "Wi-Fi Certified." May replace 802.11b. Improved security enhancements over 802.11. Compatible with 802.11b. 14 channels available in the 2.4GHz band (only 11 of which can be used in the U.S. due to FCC regulations) with only three

				non-overlapping channels.

Note: Maximum wireless signal rate based on IEEE Standard 802.11g specifications is 54 Mbps. But actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead will cause lower actual data throughput rate.

4.5.2.3 Wireless Security

Various security options are available on the Gawv5.4U4-A3 including open or WEP, 802.1x, WPA, WPA-PSK, WPA2 and WPA2-PSK. In the following, some authentications will be introduced. For details on these methods and how to use them, please read the wireless LAN configuration information in Section 1.3.2 (Wireless Security Configuration).

1. WEP is short for ***W**ired **E**quivalent **P**rivacy* (or ***W**ireless **E**ncryption **P**rotocol*), **WEP** is part of the IEEE 802.11 wireless networking standard and was designed to provide the same level of security as that of a wired LAN. Because wireless networks broadcast messages using radio, they are susceptible to eavesdropping. WEP provides security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another.

WEP was the encryption scheme considered to be the initial standard for first generation wireless networking devices. However, it has been found that WEP is not as secure as once believed. WEP is used at the two lowest layers of the OSI model - the data link and physical layers; it therefore does not offer end-to-end security.

WEP's major weakness is its use of static encryption keys. When you set up a router with a WEP encryption key, that one key is used by every device on your network to encrypt every packet that's transmitted. But the fact that packets are encrypted doesn't prevent them from being intercepted, and due to some esoteric technical flaws it's entirely possible for an eavesdropper to intercept enough WEP-encrypted packets to eventually deduce what the key is.

2. WPA is short for ***W**i-Fi **P**rotected **A**ccess*, it debuted to address many of WEP's shortcomings. It includes two improvements over WEP:

·Improved data encryption through the temporal key integrity protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.

·User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

To encrypt a network with WPA Personal/PSK you provide your router not with an encryption key, but rather with a plain-English passphrase between 8 and 63 characters long. Using a technology called TKIP (for Temporal Key Integrity Protocol), that passphrase, along with the network SSID, is used to generate unique encryption keys for each wireless client. And those encryption keys are constantly changed. (Although WEP also supports passphrases, it does so only as a way to more easily create static keys, which are usually comprised of the hex characters 0-9 and A-F).

3. The 802.1X standard is designed to enhance the security of wireless local area networks (WLANs) that follow the IEEE 802.11 standard. 802.1X provides an authentication framework for wireless LANs, allowing a user to be authenticated by a central authority. The actual algorithm that is used to determine whether a user is authentic is left open and multiple algorithms are possible.

802.1X uses an existing protocol, the Extensible Authentication Protocol (EAP, RFC 2284), that works on Ethernet, Token Ring, or wireless LANs, for message exchange during the authentication process.

In a wireless LAN with 802.1X, a user (known as the *supplicant*) requests access to an access point (known as the *authenticator*). The access point forces the user (actually, the user's client software) into an unauthorized state that allows the client to send only an EAP start message. The access point returns an EAP message requesting the user's identity. The client returns the identity, which is then forwarded by the access point to the *authentication server*, which uses an algorithm to authenticate the user and then returns an accept or reject message back to the access point. Assuming an accept was received, the access point changes the client's state to authorized and normal traffic can now take place.

The authentication server may use the Remote Authentication Dial-In User Service (RADIUS),

although 802.1X does not specify it.

4. WPS is short for Wi-Fi Protected Setup, was introduced and developed by the Wi-Fi Alliance (http://www.wi-fi.org/) to help standardize and simplify ways of setting up and configuring security on a wireless network. Traditionally, users would have to manually create a wireless network name (SSID), then manually enter a creative, yet predictable security key on both the access point and the client to prevent unwanted access to their wireless network. This whole process requires the users to have the background knowledge of the Wi-Fi devices and the ability to make the necessary configuration changes. WPS was introduced to relieve and remove all of the guess work of securing a wireless network by typing a short PIN (numeric code) or pushing a button (Push-Button Configuration, or PBC). On a new wireless network, WPS will automatically configure a wireless network with a network name (SSID) and strong WPA data encryption and authentication. Wi-Fi Protected Setup is designed to support various Wi-Fi certified 802.11 products ranging from access points, wireless adapters, Wi-Fi phones, and other consumer electronics devices.

Advantages of WPS:

1. WPS automatically configures the network name (SSID) and WPA security key for the access point and the WPS enabled client devices on a network.
You do not need to know the SSID and security keys or pass phrases when connecting WPS-enabled devices.

2. No one can guess or figure out your security keys or pass phrase because the keys will be randomly generated. No predictable pass phrases or long sequences of hexadecimal to enter Information and network credentials are securely exchanged over the air using the Extensible Authentication Protocol (EAP), one of the authentication protocols used in WPA2.

3. WPS has been integrated and supported in Windows Vista (currently, Windows Vista only work in Registrar mode)

Disadvantages of WPS:

1. It does not support Ad-Hoc mode or network where wireless devices are communicated directly to each other without an access point. All of the Wi-Fi devices on the network must be WPS certified or WPS-compatible, otherwise you will not be able to take advantage of the ease of securing the network.

2. Difficult to add a non-WPS client device to the network because of the long sequences of hexadecimal characters generated by the WPS technology.
This technology is fairly new, so not every vendor will support the WPS technology.

4.5.2.4 Wireless Client requirements

4.5.2.4.1 Radio Transmission

Wireless LAN or WLAN devices use electromagnetic waves within a broad, unlicensed range of the radio spectrum to transmit and receive radio signals. When a wireless access point is present, it becomes a base station for the WLAN nodes in its broadcast range. WLAN nodes transmit digital data using FM (frequency modulation) radio signals. WLAN devices generate a carrier wave and modulate this signal using various techniques. Digital data is superimposed onto the carrier signal. This radio signal carries data to WLAN devices within range of the transmitting device. The antennae of WLAN devices listen for and receive the signal. The signal is demodulated and the transmitted data extracted. The transmission method used by the access point is called Direct Sequence Spread Spectrum (DSSS) and operates in a range of the radio spectrum between 2.4GHz and 2.5GHz for transmission. See the expert technical specifications for more details on wireless operation.

4.5.2.4.2 Antennas

Direct the external antenna to allow optimization of the wireless link. If for example the antenna is erect, wireless links in the horizontal plane are favoured. Please note that the antenna characteristics are influenced by the environment, that is by reflections of the radio signal against walls or ceilings. It is advisable to use the received signal strength as indicated by the wireless client manager to optimize the

antenna position for the link to a given client. Concrete walls weaken the radio signal and thus affect the connection.

4.5.2.4.3 Range

Range should not be a problem in most homes or small offices. If you experience low or no signal strength in some areas, consider positioning the Router in a location between the WLAN devices that maintains a roughly equal straight-line distance to all devices that need to access the Router through the wireless interface. Adding more 802.11g access points to rooms where the signal is weak can improve signal strength. Read the section about placement of the Router titled Location in the next chapter, Hardware Installation, for more information.

4.5.2.4.4 Radio channels

The 802.11g standard allows several WLAN networks using different radio channels to be co-located. The Gawv5.4U4-A3 supports multiple radio channels and is able to select the best radio channel at each startup. You can choose to set the channels automatically or manually.
The different channels overlap. To avoid interference with another access point, make sure that the separation (in terms of frequency) is as high as possible. It is recommended to keep at least 3 channels between 2 different access points.
The Gawv5.4U4-A3 supports all channels allowed for wireless networking. However, depending on local regulations, the number of channels actually allowed to be used may be additionally restricted, as shown in the table below.

Regulatory Domain	Allowed Radio Channels
China	**1 to 13**
Europe	**1 to 13**
Israel	**5 to 8**
Japan	**1 to 14**
Jordan	**10 to 13**
Thailand	**1 to 14**
USA / Canada	**1 to 11**

4.5.2.5 Wireless Distribution System

The WL series of APs use wireless ports to interconnect BSS areas. WDS is commonly used in areas requiring multiple APs, where wiring is not possible or costly and for providing back-up paths between APs. The number of ports on an AP available for the WDS is dependent on the AP model. The 520wl for example, allows up to six WDS links. The same frequency channels must be used on each end of a WDS link. The same PC card that supports a BSS area can be used for a WDS link. The packet flow through the WDS is very similar to the standard DS except it uses the wireless ports instead of the Ethernet port.

4.5.3 Configure Wireless Connection

4.5.3.1 Wireless – Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name

(also known as SSID) and restrict the channel set based on country requirements.

Following is a description of the different options:

- **Enable Wireless**: If you want to make wireless be available, you have to check this box first. Otherwise, the Hide Access Point SSID, Country, Enable Wireless Guest Network, and Guest SSID box will not be displayed.
- **Hide Access Point**: Check this box if you want to hide any access point for your router, so a station cannot obtain the SSID through passive scanning.
- **Clients Isolation:** When many clients connect to the same access point, they can access each other. If you want to disable the access between clients which connect the same access point, you can check this box.
- **Disable WMM Advertise:** WMM is short for wi-fi multimedia, which can provide high-performance multimedia voice、video data transfers.
- **SSID**: The SSID is the network name shared among all points in a wireless network. The SSID must be identical for all points in the wireless network. It is case-sensitive and must not exceed 32 characters (use any of the characters on the keyboard). Make sure this setting is the same for all points in your wireless network. For added security, you should change the default SSID to a unique name.
- **Country:** The name of the country with which your gateway is configured. This parameter further specifies your wireless connection. For example, The channel will adjust according to nations to adapt to each nation's frequency provision.
- **Max Clients:** Specifies maximum wireless client stations to be enble to link with AP. Once the clients exceed the max vlaue, all other clients will be refused. The value range is between six and ten.
- **Wireless - Guest/Virtual Access Points:** If you want to make Guest/Virtual network function be available, you have to check those boxes in the table below. In the current software version, three virtual access points can be configured.
- **Guest AP Configuration**: The configuration is the same as the main SSID (Service Set Identification), has the unique name, the limit of clients, and so on.

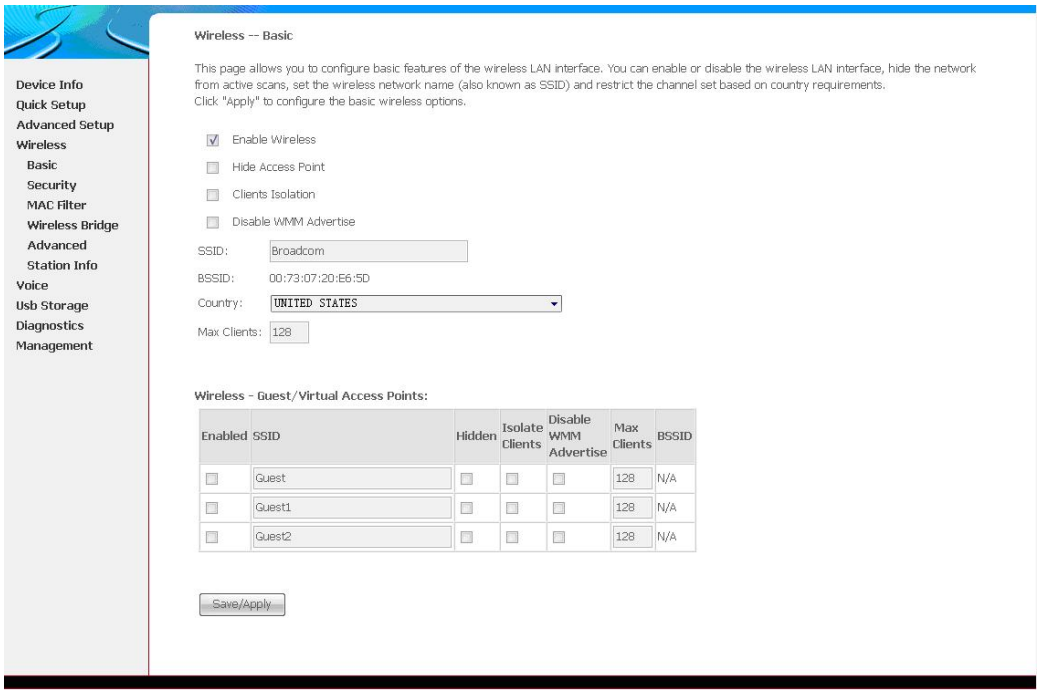


Figure3.1.6: Wireless—Basic

Click "Save/Apply" to save the basic wireless options and make the change take effect.

4.5.3.2 Wireless – Security

This page allows you can configure security features of the wireless LAN interface. You can sets the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
This device is equipped with 802.1X and WPA/WPA2 (Wi-Fi Protected Access), the latest security standard. It also supports the legacy security standard, WEP (Wired Equivalent Privacy). By default, wireless security is disabled and authentication is open. Before enabling the security, consider your network size, complexity, and existing authentication infrastructure and then determine which solution applies to it.
Following is a description of the different options:

- **Select SSID:** Select the wireless LAN of SSID to configure security features.

- **No Encryption :** Please refer to below for details of configuration

Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be open.
WEP Encryption: Disable WEP Encryption.
The data is not encrypted when it is transferred from the device to the client station. This is the default option.

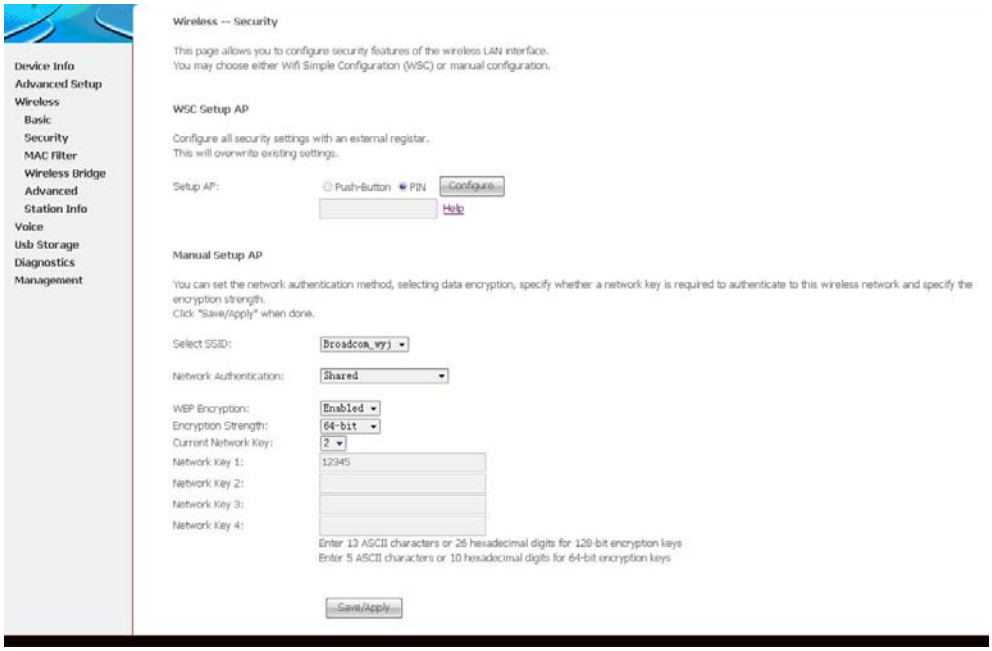


Figure3.1.7:Wirless –security(No Encryption)

Click "Save/Apply" to save the wireless security options and make the change take effect.

- **64-bit WEP :** Please refer to below for details of configuration

  Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be open or shared.

  WEP Encryption: Enable WEP Encryption.

  Encryption Strength: click the desired Data Security level to be 64-bit.

  Current Network Key: Select one of network key that you set on the Key boxes as default one.

  Network Key 1 to 4: Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys to fill out WEP keys box. The system allows you to type in 4 kinds of the WEP key.

Click "Save/Apply" to save the wireless security options and make the change take effect.

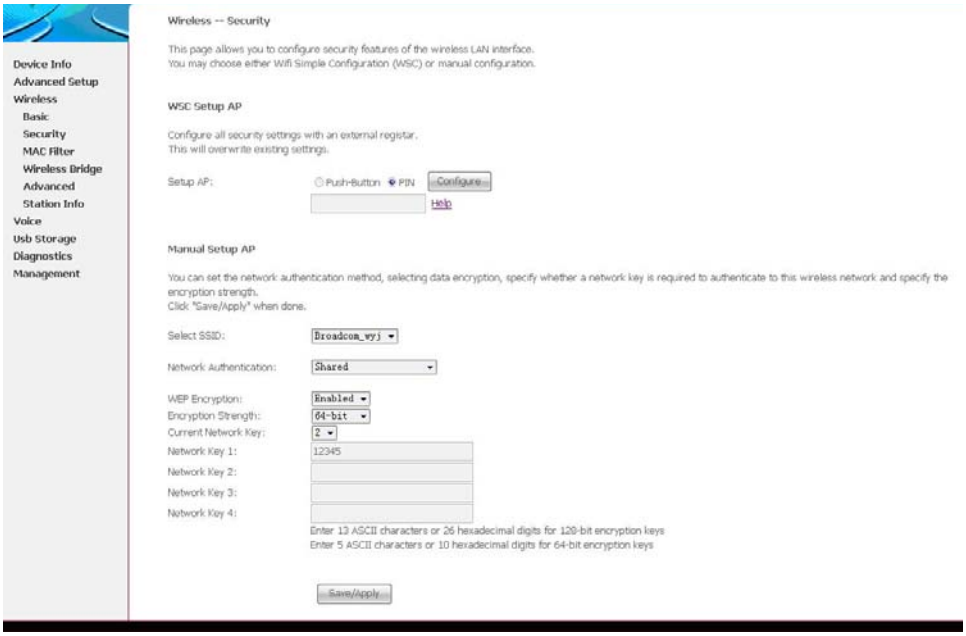


Figure3.1.8: Wireless—Security(64-bit WEP)

- **128-bit WEP :** Please refer to below for details of configuration

Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be open or shared.

WEP Encryption: Enable WEP Encryption.

Encryption Strength: click the desired Data Security level to be 128-bit.

Current Network Key: Select one of network key that you set on the Key boxes as default one.
Network Key 1 to 4: Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys to fill out WEP keys box. The system allows you to type in 4 kinds of the WEP key.
Click "Save/Apply" to save the wireless security options and make the change take effect.

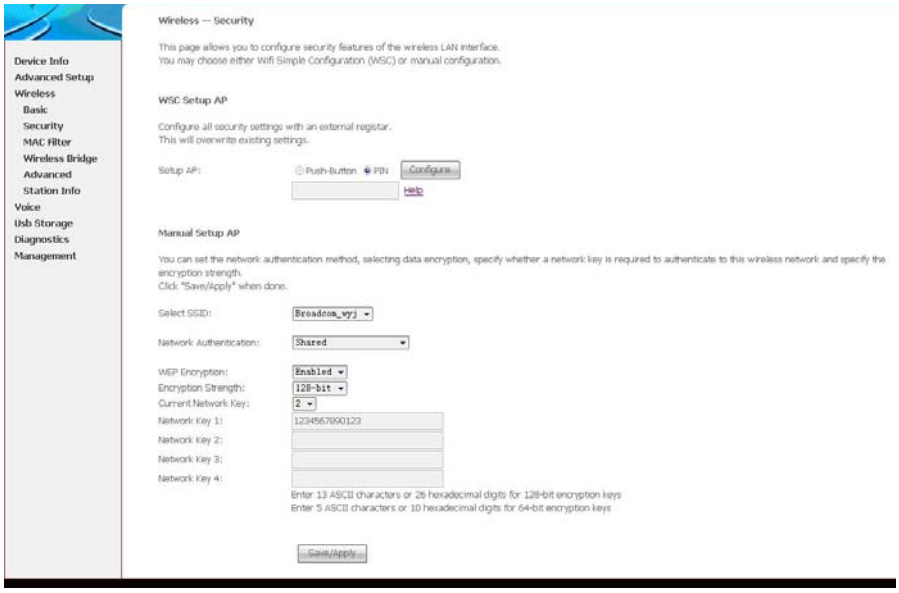


Figure3.1.9:Wireless—Security(128-bit WEP)

Before introducing the following authentications, you need to understand the radius server.

RADIUS server is short for A Remote Authentication Dial-in User Service server, which is most commonly a third party server, used for authentication of wireless clients who wish to connect to an access point. The wireless client contacts an access point (a RADIUS client), which in turn communicates with the RADIUS server. The RADIUS server performs the authentication by verifying

the client's credentials, to determine whether the device is authorized to connect to the access point's LAN. If the RADIUS server accepts the client, it responds by exchanging data with the access point, including security keys for subsequent encrypted sessions. A typical topology which adopt the radius server see figure:

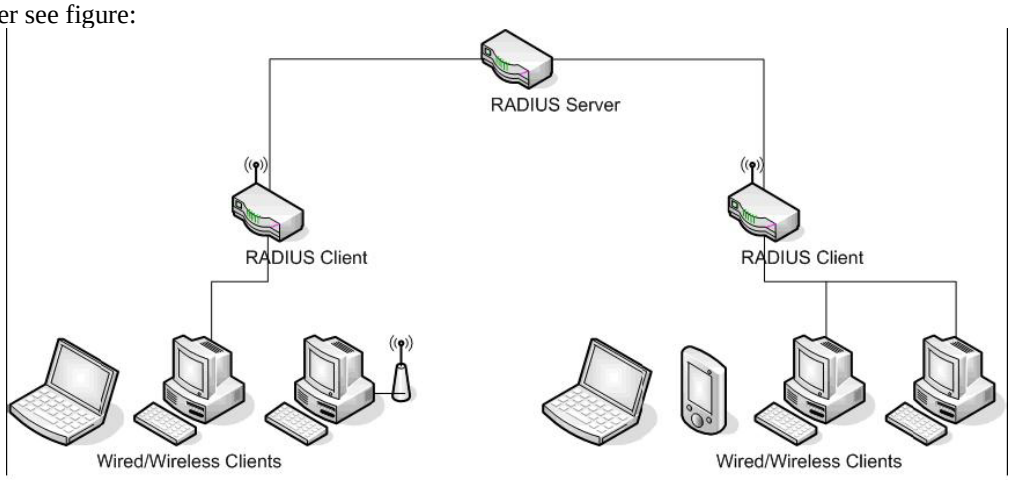


Figure 8 adopting radius server authenction topology

- **802.1x Authentication:** Please refer to below for details of configuration

Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be 802.1x.

Radius Server IP Adress: Enter the IP Address of the authentication server.
Radius Port: Enter the port number of the authentication server. The default port number is 1812.
Radius Key: Enter the same key as the Radius server's.
WEP Encryption: Enable WEP Encryption. This is default

Encryption Strength: click the desired Data Security level to be 64-bit or 128-bit.

Current Network Key: Select one of network key that you set on the Key boxes as default one.
Network Key 1 to 4: Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys or enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys to fill out WEP keys box. The system allows you to type in 4 kinds of the WEP key.
Click "Save/Apply" to save the wireless security options and make the change take effect.

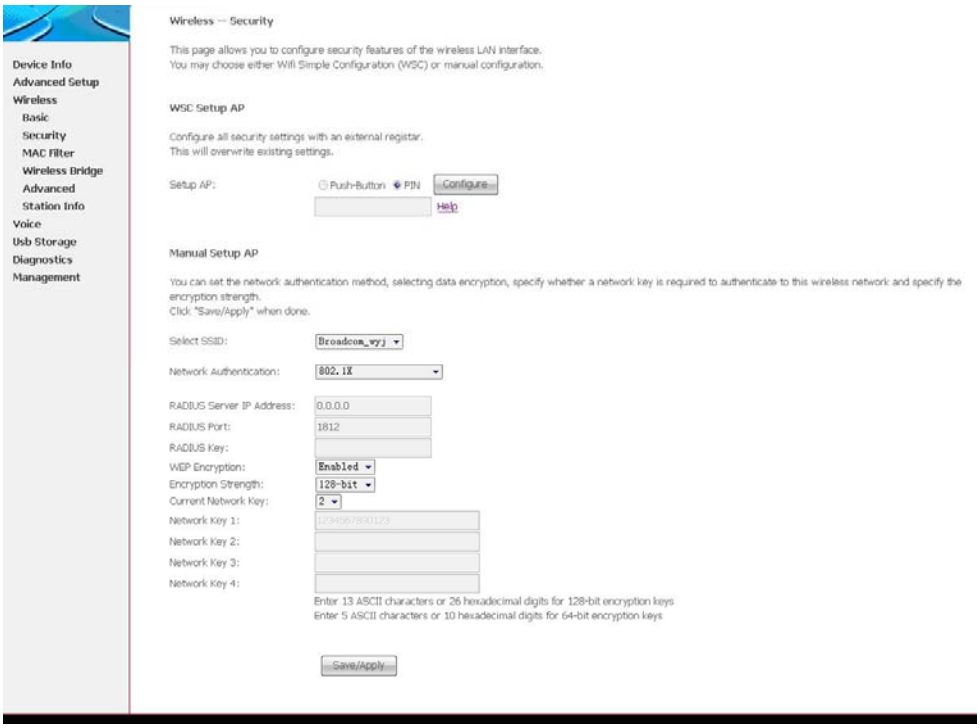


Figure3.1.10: Wireless—Security(802.1x Authentication**)**

- **WPA Authentication:** Please refer to below for details of configuration

Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be WPA.

WPA Group Rekey Interval: Specifies the timer the WPA key must change. If the value set 0, no need to change. The change is done automatically between the server and the client.
Radius Server IP Adress: Enter the IP Address of the authentication server.
Radius Port: Enter the port number of the authentication server. The default port number is 1812.
Radius Key: Enter the same key as the Radius server's.
WPA Encryption: Select TKIP, AES or TKIP + AES. The TKIP is default. The TKIP + AES encryption mode means AP auto adjust to use TKIP or AES according to wireless clients.
Click "Save/Apply" to save the wireless security options and make the change take effect.

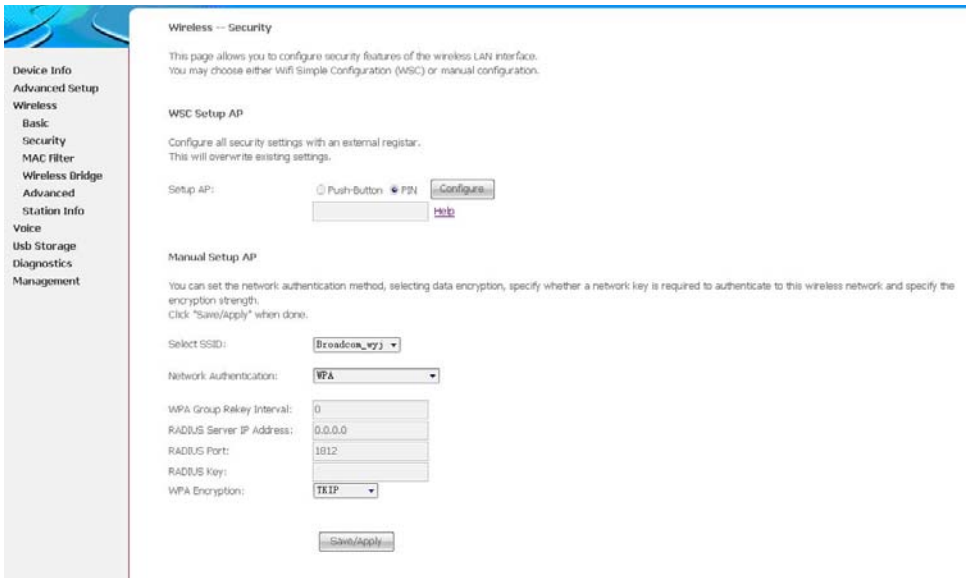


Figure3.2.1:Wireless—Security(WPA Authentication)

- **WPA2 Authentication:** Please refer to below for details of configuration

Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be WPA2.

WPA2 Preauthentication: Selec Enable or Disenable.

Network Re-auth Interval: Specifies the timer of re-authentication between the server and the client.
WPA Group Rekey Interval: Specifies the timer the WPA key must change. If the value set 0, no need to change. The change is done automatically between the server and the client.
Radius Server IP Adress: Enter the IP Address of the authentication server.
Radius Port: Enter the port number of the authentication server. The default port number is 1812.
Radius Key: Enter the same key as the Radius server's.
WPA Encryption: Select TKIP, AES or TKIP + AES. The AES is default. The TKIP + AES encryption mode means AP auto adjust to use TKIP or AES according to wireless clients.
Click "Save/Apply" to save the wireless security options and make the change take effect.

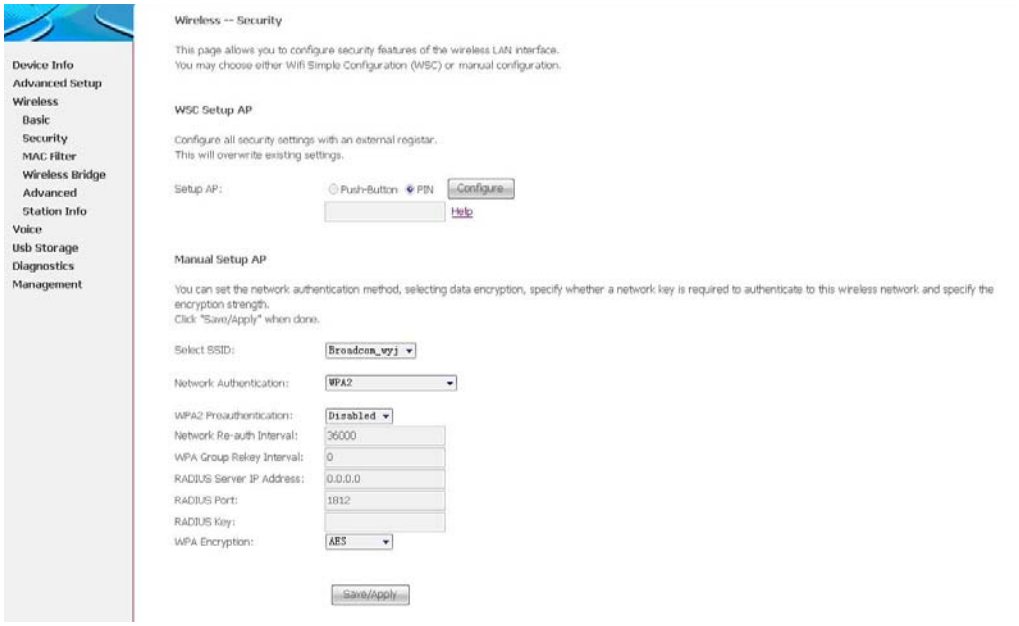


Figure3.2.2: Wireless—Security(WPA2 Authentication)

- **Mixed WPA2/WPA Authentication:** This authentication mode means AP auto adjust to use WPA2 or WPA according to wireless clients. Please refer to below for details of configuration

Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be Mixed WPA2/WPA.

WPA2 Preauthentication: Selec Enable or Disenable.
Network Re-auth Interval: Specifies the timer of re-authentication between the server and the client.
WPA Group Rekey Interval: Specifies the timer the WPA key must change. If the value set 0, no need to change. The change is done automatically between the server and the client.
Radius Server IP Adress: Enter the IP Address of the authentication server.
Radius Port: Enter the port number of the authentication server. The default port number is 1812.
Radius Key: Enter the same key as the Radius server's.
WPA Encryption: Select TKIP, AES or TKIP + AES. The AES is default. The TKIP + AES encryption mode means AP auto adjust to use TKIP or AES according to wireless clients.

Click "Save/Apply" to save the wireless security options and make the change take effect.

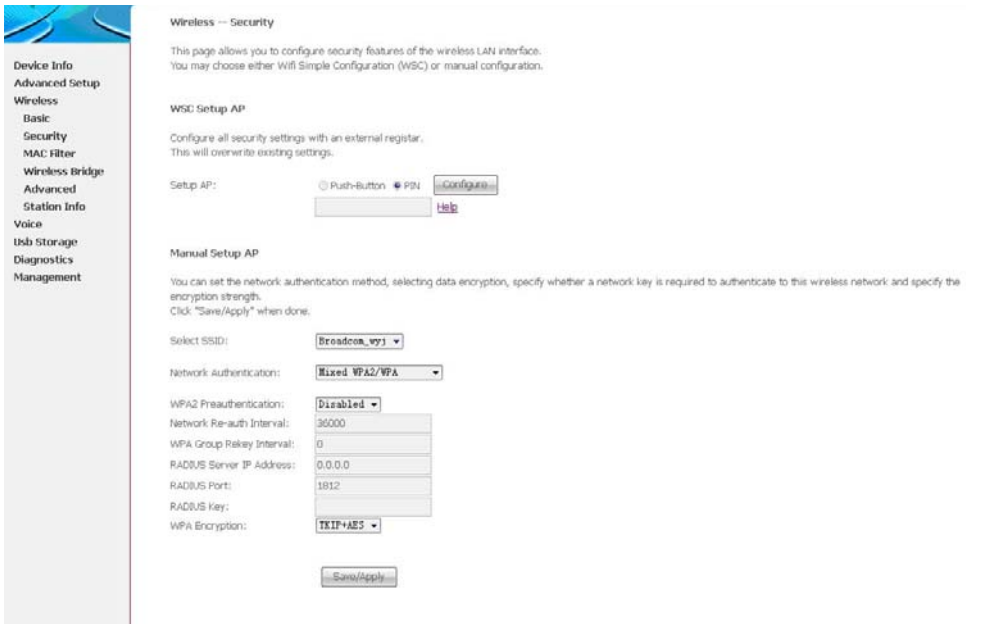


Figure3.2.3:Wireless—Security(Mixed WPA2/WPA Authentication)

- **WPA-PSK Authentication:** Please refer to below for details of configuration

Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be Mixed WPA-PSK.

WPA Pre-Shared Key: Enter the pre-shared key for WPA. Client stations must use the same key in order to connect with this device. Check the table below for instructions when entering the key.

Format	Minimum characters	Maximum Characters
ASCII	8	63
Hexadecimal	8	64

WPA Group Rekey Interval: Specifies the timer the WPA key must change. If the value set 0, no need to change. The change is done automatically between the server and the client.

WPA Encryption: Select TKIP, AES or TKIP + AES. The TKIP is default. The TKIP + AES encryption mode means AP auto adjust to use TKIP or AES according to wireless clients.

Click "Save/Apply" to save the wireless security options and make the change take effect.

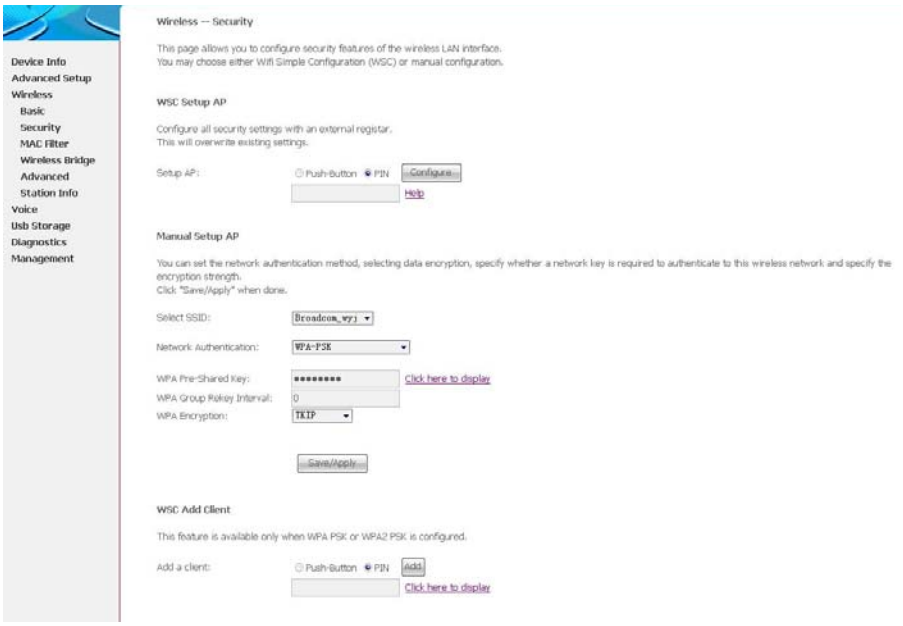


Figure3.2.4: Wireless—Security(WPA-PSK Authentication**)**

- **WPA2-PSK Authentication:** Please refer to below for details of configuration

Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be Mixed WPA2-PSK.

WPA Pre-Shared Key: Enter the pre-shared key for WPA. Client stations must use the same key in order to connect with this device. Check the table below for instructions when entering the key.

Format	Minimum characters	Maximum Characters
ASCII	8	63
Hexadecimal	8	64

WPA Group Rekey Interval: Specifies the timer the WPA key must change. If the value set 0, no need to change. The change is done automatically between the server and the client.

WPA Encryption: Select TKIP, AES or TKIP + AES. The AES is default. The TKIP + AES encryption mode means AP auto adjust to use TKIP or AES according to wireless clients.

Click "Save/Apply" to save the wireless security options and make the change take effect.

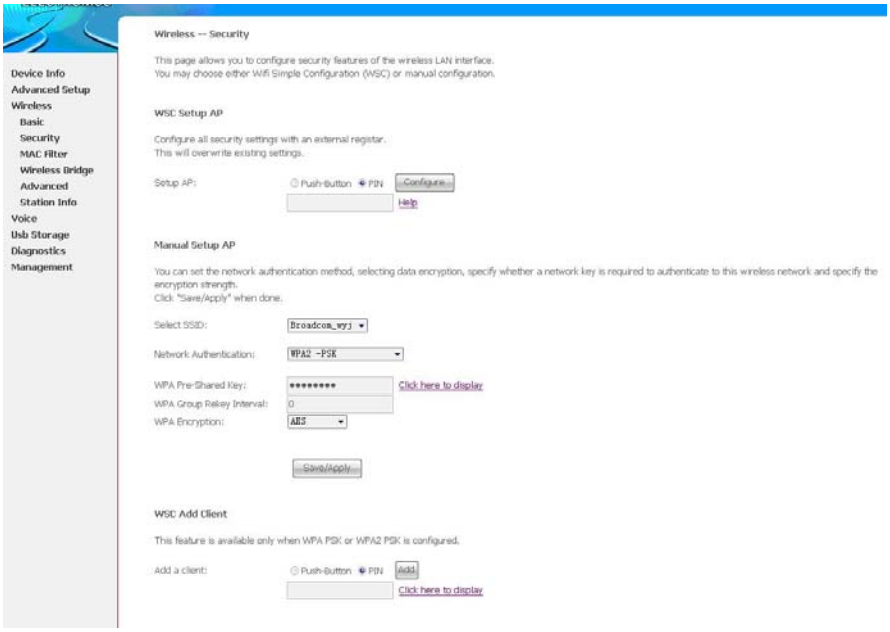


Figure 3.2.5: Wireless—Security(WPA2-PSK Authentication)

- **Mixed WPA2/WPA-PSK Authentication:** This authentication mode means AP auto adjust to use WPA2-PSK or WPA-PSK according to wireless clients. Please refer to below for details of configuration

Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be Mixed WPA2/WPA-PSK.

WPA Pre-Shared Key: Enter the pre-shared key for WPA. Client stations must use the same key in order to connect with this device. Check the table below for instructions when entering the key.

Format	Minimum characters	Maximum Characters
ASCII	8	63
Hexadecimal	8	64

WPA Group Rekey Interval: Specifies the timer the WPA key must change. If the value set 0, no need to change. The change is done automatically between the server and the client.

WPA Encryption: Select TKIP, AES or TKIP + AES. The AES is default. The TKIP + AES encryption mode means AP auto adjust to use TKIP or AES according to wireless clients.

Click "Save/Apply" to save the wireless security options and make the change take effect.

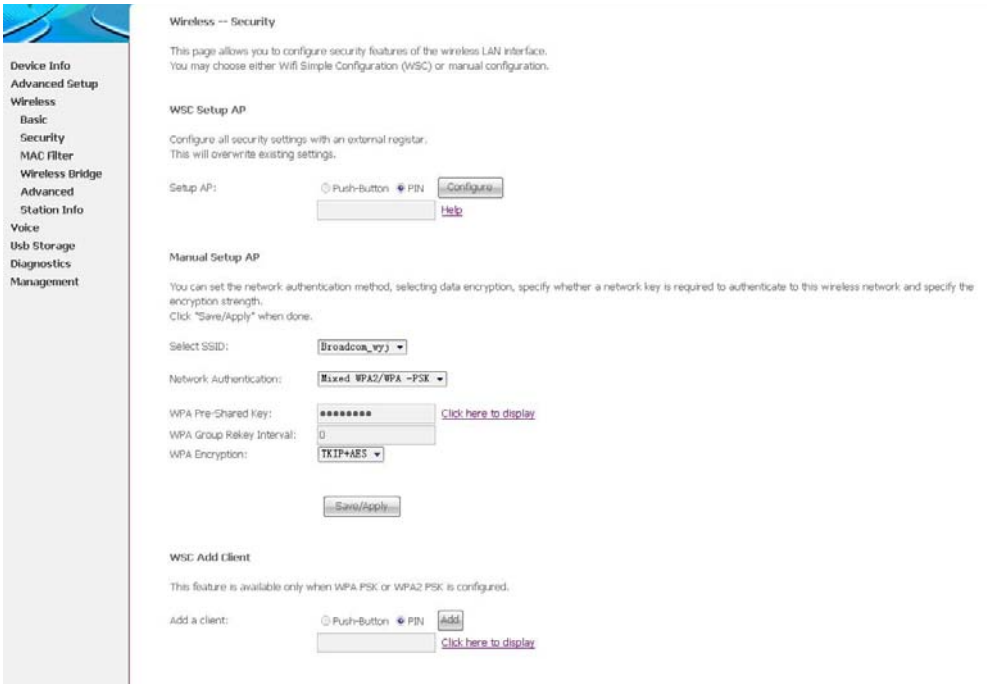


Figure 3.2.6:Wireless—Security(Mixed WPA2/WPA-PSK Authentication)

- **Mixed WPA2/WPA Authentication:** This authentication mode means AP auto adjust to use WPA2-PSK or WPA-PSK according to wireless clients. Please refer to below for details of configuration

Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be Mixed WPA2/WPA.

WPA Pre-Shared Key: Enter the pre-shared key for WPA. Client stations must use the same key in order to connect with this device. Check the table below for instructions when entering the key.

Format	Minimum characters	Maximum Characters
ASCII	8	63
Hexadecimal	8	64

WPA2 Preauthentication: Selec Enable or Disenable.
Network Re-auth Interval: Specifies the timer of re-authentication between the server and the client.
WPA Group Rekey Interval: Specifies the timer the WPA key must change. If the value set 0, no need to change. The change is done automatically between the server and the client.
Radius Server IP Adress: Enter the IP Address of the authentication server.
Radius Port: Enter the port number of the authentication server. The default port number is 1812.
Radius Key: Enter the same key as the Radius server's.
WPA Encryption: Select TKIP, AES or TKIP + AES. The AES is default. The TKIP + AES encryption mode means AP auto adjust to use TKIP or AES according to wireless clients.

Click "Save/Apply" to save the wireless security options and make the change take effect.

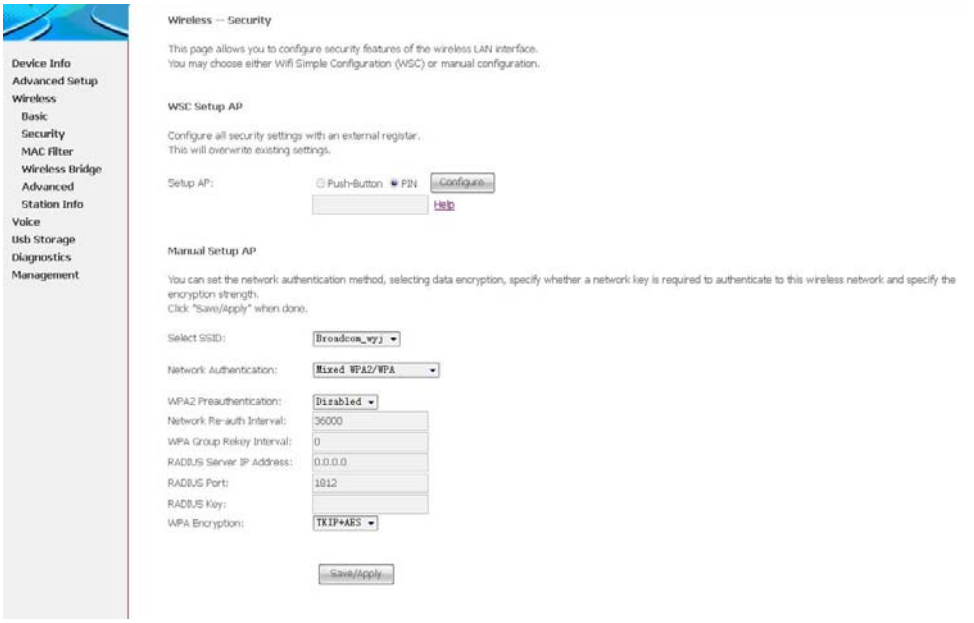


Figure3.2.7: Wireless—Security(Mixed WPA2/WPA Authentication)

- **WPS Authentication:** There are 2 primary methods used in the Wi-Fi Protected Setup:

  1、PIN entry, a mandatory method of setup for all WPS certified devices

  2、Push button configuration (PBC), an actual push button on the hardware or through a simulated push button in the software. (This is an optional method on wireless client).

If you are using the PIN method, you will need a Registrar (access point/wireless router) to initiate the registration between a new device and an active access point/wireless router. (Note: The PBC method may also need a Registrar when used in a special case where the PIN is all zeros)

In order to use wps authentication, you must ensure netcard support the function, if it support, you don't need to do any configuration. Only need to do is to press the wps button to enable the wps function.

4.5.3.3 Wireless-MAC Filter

The web page allows you to create a list of MAC addresses that are banned or allowed association with the wireless access point

- **MAC Restrict Mode: The function can be turn on/off,** Check on **Disabled** to disable this function. Vice versa, to enable the function. After enabling the function, you can filter wireless users according to their MAC address, either allowing or denying access. Check on **Allow** to make any wireless MAC address in the Wireless Access Control List can be linked to. And Check on **Deny** to banned any wireless MAC address in the Wireless Access Control List to be linked to.

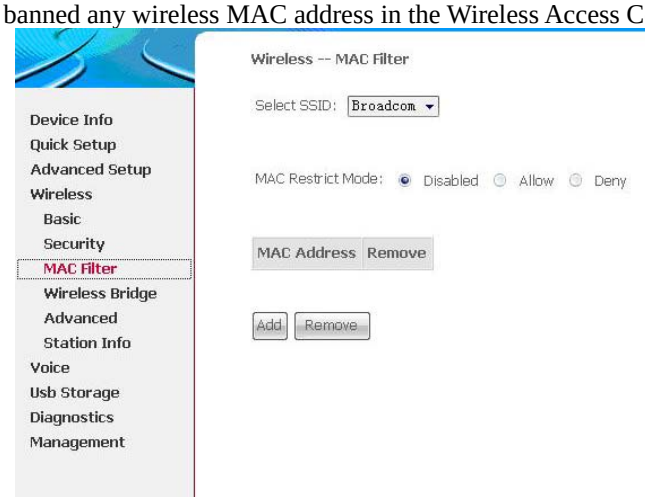


Figure 3.2.8:Wireless-MAC filter

- **Add a MAC Access Control:** To add a new MAC address to your wireless MAC address filters, click on the Add button to show next page. Type in the MAC Address in the entry field provided. Click the Save/Apply button to add the MAC address to the list. The MAC address will appear listed in the table below.

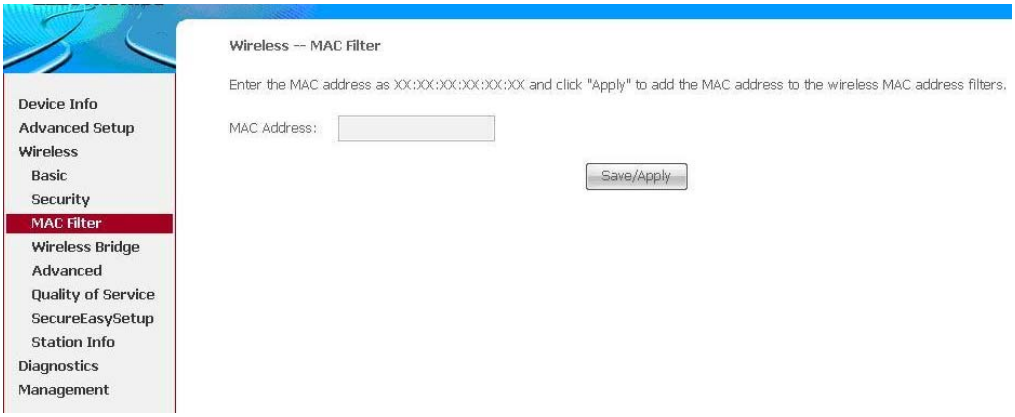


Figure 3.2.9:Wireless—MAC filter(ADD)

- **Remove a MAC Access Control:** Check on the remove box in the right column of the list for the MAC address to be removed and then click Remove button.

4.5.3.4 Wireless – Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface.

The Wireless Distribution System (WDS) allows you to extend the range of your wireless network by introducing one or more WDS-enabled devices into your wireless network. You can only establish WDS links with WDS-enabled devices.

- **AP Mode:** Select Access Point's functionality to be Access Point or pure Wireless Bridge. You can select Wireless Bridge (also known as Wireless Distribution System) to disables access point functionality. Selecting Access Point enables access point functionality and Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP.
- **Bridge Restrict:** Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.

You can manually input Remote Bridges MAC Address to the list. Also you can do it automatically. Proceed as follows:

- In the **Bridge Restrict** list, click Enabled(Scan).
- Click "Refresh" to update the remote bridges.

The Gawv5.4U4-A3 will Wait for few seconds to update. And then lists the results in the Accessible Access Points table.

- Check on the box in the left column of the list for selecting the Access Point to which you want to establish a WDS connection.
- Click Save/Apply.

You must configure all Bridges Access Point with:

- The same encryption and authentication mode as Open, Shared, WEP, WPA-PSK or WPA2-PSK.
- The same fixed channel.

Click "Save/Apply" to configure the wireless bridge options and make the change take effect.

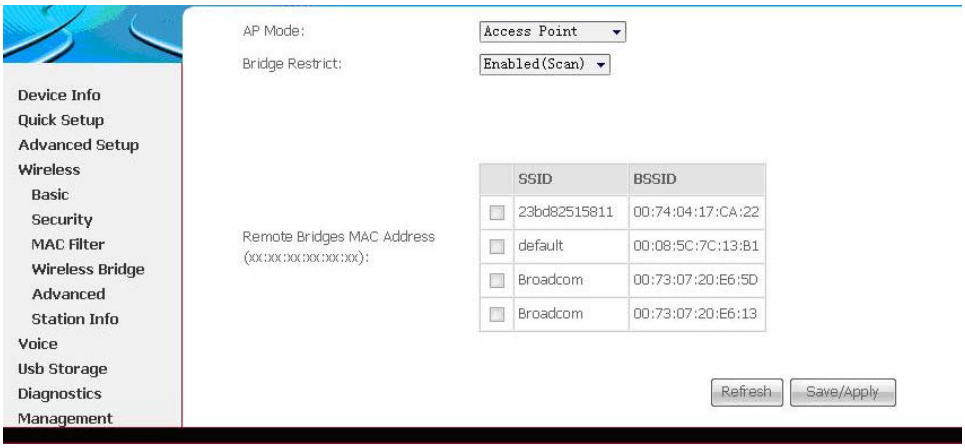


Figure3.2.10: Wireless--Bridge

4.5.3.5 Wireless – Advanced

This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.

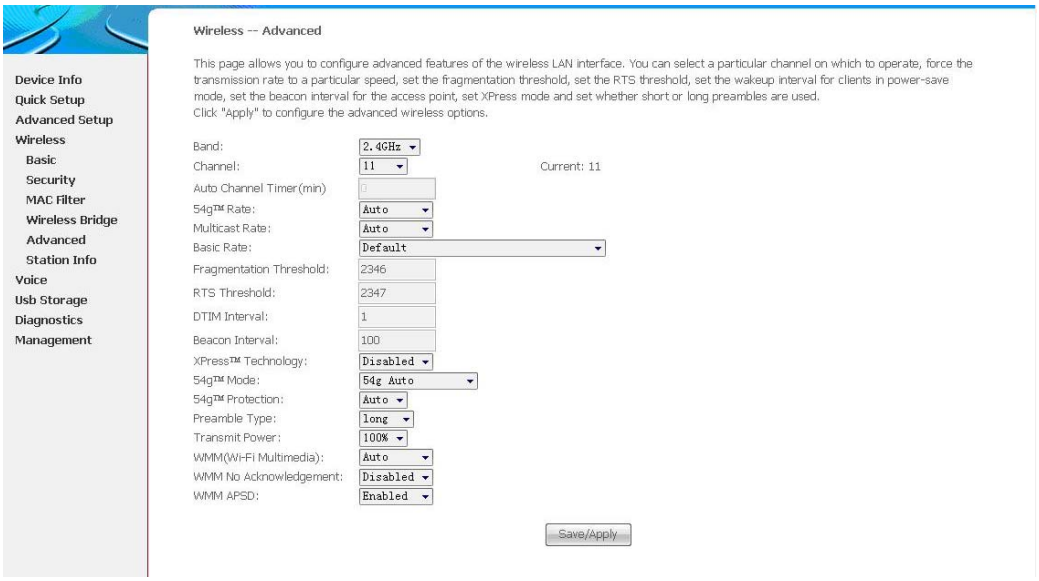


Figure3.3.1: Wireless—Advanced

- **Band:** Select 802.11b/g using wireless frequency band range. The radio frequency will remain at 2.437GHz.
- **Channel:** Fill in the appropriate channel to correspond with your network settings. 11 is the default channel. All devices in your wireless network must use the same channel in order to work correctly. This router supports auto channelling functionalty.
- **Auto Channel Timer(min):** Specifies the timer of auto channelling.
- **54g™ Rate:** Select the transmission rate for the network. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **Auto** to have the Router automatically use the fastest possible data rate

and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is **Auto**.

- **Multicast Rate:** Select the multicast transmission rate for the network. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **Auto** to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is **Auto**.
- **Basic Rate:** Select the basic transmission rate ability for the AP.
- **Fragmention Threshold:** Packets that are larger than this threshold are fragmented into multiple packets. Try to increase the fragmentation threshold if you encounter high packet error rates. Do not set the threshold too low, since this can result in reduced networking performance.
- **RTS Threshold:** This value should remain at its default setting of 2347.Should you encounter inconsistent data flow, only minor reductions are recommended. Should you encounter inconsistent data flow, only minor reduction of the default value, 2347, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of 2347.
- **DTIM Interval:** (Delivery Traffic Indication Message) Enter a value between 1 and 255 for the Delivery Traffic Indication Message (DTIM.) A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.
- **Beacon Interval:** A beacon is a packet of information that is sent from a connected device to all other devices where it announces its availability and readiness. A beacon interval is a period of time (sent with the beacon) before sending the beacon again. The beacon interval may be adjusted in milliseconds (ms). Default (100) is recommended.
- **XPress™ Technology:** Select Enable or Disable. This is a special accelerating technology for IEEE802.11g. The defaule is Disabled.
- **54g™ Mode:** Compatible with IEEE 802.11b, IEEE 802.11g. Select a Standards from the drop-down list box. Its default setting is 54g Auto. The drop-down list box includes below mode:

802.11b Only
Only stations that are configured in 802.11b mode can associate. If you select it, the rate of transmission **will only has selected value: 1Mbps、2Mbps、5.5Mbps、11Mbps. For other selections,** the rate of transmission will has lots of selected value: 1Mbps、2Mbps、5.5Mbps、6Mbps、9Mbps、11Mbps、12Mbps、18Mbps、24Mbps、36Mbps、48Mbps、54Mbps.
54g LRS
This is a special compatibility mode for 802.11b/g and is in fact designed for older types of b-clients. Use this mode if you are experiencing problems with wireless clients that connect to the Gawv5.4U4-A3 Access Point. If you select it, the preamble type will be disabled, which can't be set.
54g Auto
Only stations that are configured in 802.11b/g mode can associate.
54g Perfomance
Only stations that are configured in 802.11g mode can associate. It is the same as 54g LRS, if you select it, the preamble type will be disabled, which can't be set.

- **54g™ Protection:** The 802.11g standards provide a protection method so 802.11g and 802.11b devices can co-exist in the same network without "speaking" at the same time. Do not disable 54g Protection if there is a possibility that a 802.11b device may need to use your wireless network. In Auto Mode, the wireless device will use RTS/CTS to improve 802.11g performance in mixed 802.11g/802.11b networks. Turn protection off to maximize 802.11g throughput under most conditions.

- **Preamble Type:** Preambles are a sequence of binary bits that help the receivers synchronize and ready for receipt of a data transmission. Some older wireless systems like 802.11b implementation use shorter preambles. If you are having difficulty connecting to an older 802.11b device, try using a short preamble. You can select short preamble on if the 54g mode is set to 802.11b Only in the 54g Mode field.
- **Transmit Power:** Adjust the transmission range here. This tool can be helpful for security purposes if you wish to limit the transmission range.
- WMM(Wi-Fi Multimedia):Select whether WMM is enable or disabled. **Before you disable WMM, you should understand that all qos queues、traffic classes relate to wireless will not take effects.**

· **WMM No Acknowledgement:** Select whether ACK in WMM packet. By default, the 'Ack Policy' for each access category is set to Disable, meaning that an acknowledge packet is returned for every packet received. This provides a more reliable transmission but increases traffic load, which decreases performance. To disable the acknowledgement can be useful for Voice, for example, where speed of transmission is important and packet loss is tolerable to a certain degree.

- WMM APSD: APSD is short for automatic power save delivery, Selecting enable will make it has very low power consumption. WMM Power Save is an improvement to the 802.11e amendment adding advanced power management functionality to WMM.

Click "Save/Apply" to configure the advanced wireless options and make the change take effect.

4.5.3.6 Queue Config

This page allows you to configure WMM(Wi-Fi Multimedia) features of the wireless LAN interface. Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance certification, based on the IEEE 802.11e draft standard. It provides basic Quality of Service (QoS) features to IEEE 802.11 networks.
In the Queue Config web page, the queue about wireless which have eight -predefined queues can’t be edited, see figure:

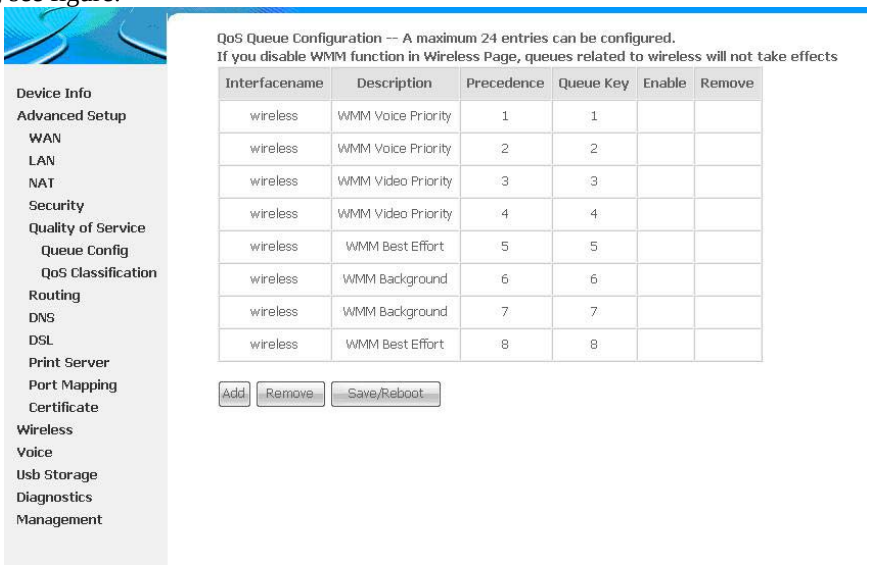


Figure3.3.2:Wireless—Queue Config

From the figure, we can see that Background, Best Effort, Video and Voice are access categories for packet prioritization. Upon enabling WMM,the highest priority is given to Voice packets, decreasing towards Background packets which receive the lowest priority.

4.5.3.7 Qos Classification

WMM or Wi-Fi MultiMedia enhances QoS at wireless driver level. It provides a mechanism to prioritize wireless data traffic to and from the associated (WMM capable) stations. Network traffic

classes is automatically assigned according to DSCP in TCP/IP header. Extended Wireless QoS Classification can choose Add QoS Entry or Remove QoS Entry to configure
In the Add/Edit Wireless Quality of Service Rule WEB interface, you can edit a rule consists of a class name , Wireless Transmit Priority and at least one condition as Protocol, Source IP Address, Source Subnet Mask, UDP/TCP Source Port (port or port:port), Destination IP Address, Destination Subnet Mask and UDP/TCP Destination Port(port or port:port). All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the rule.

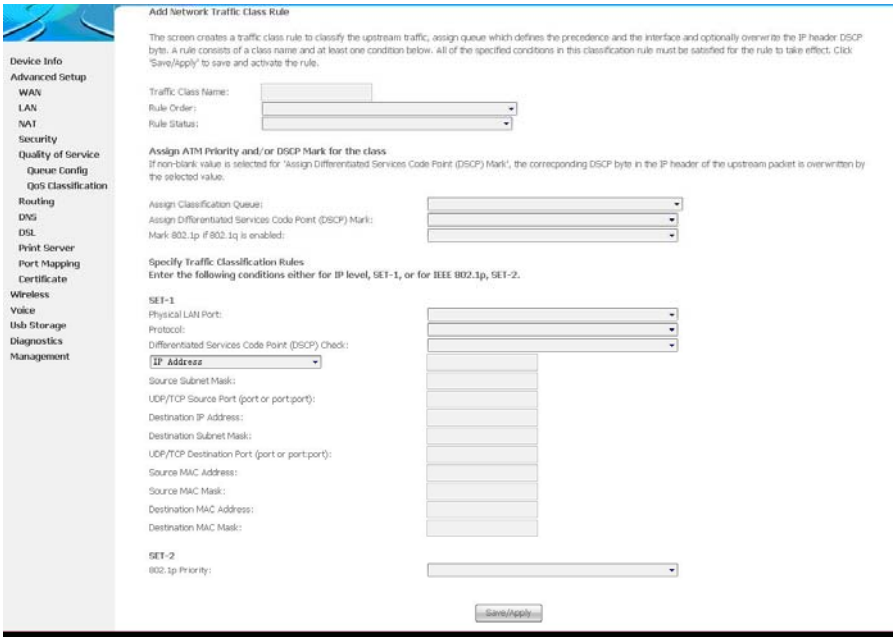


Figure 3.3.3:Wireless—Qos Classification(ADD)

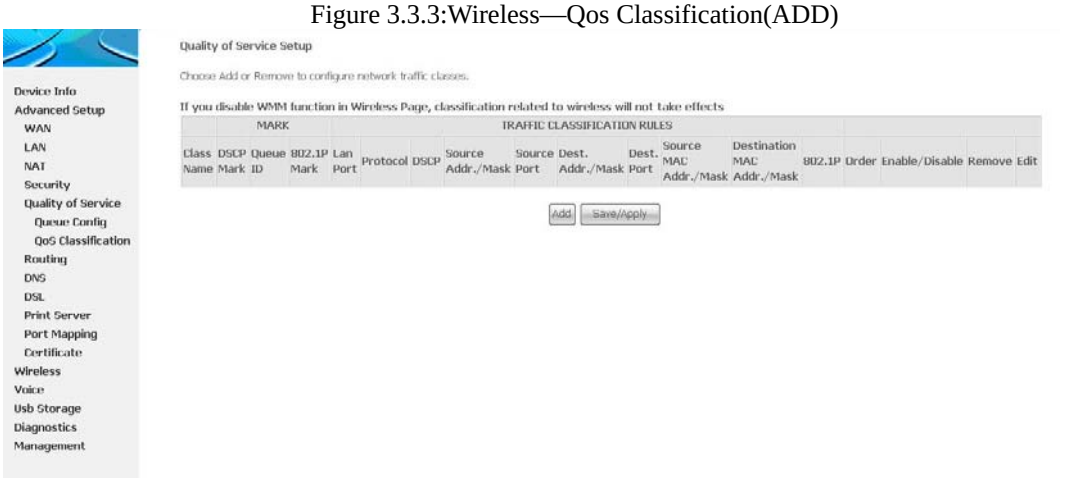


Figure 3.3.4: Wireless—Qos Classification

In the last, click "Save/Apply" to configure the wireless QOS options and make the change take effect.

4.5.3.8 Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status about Association and authentication.

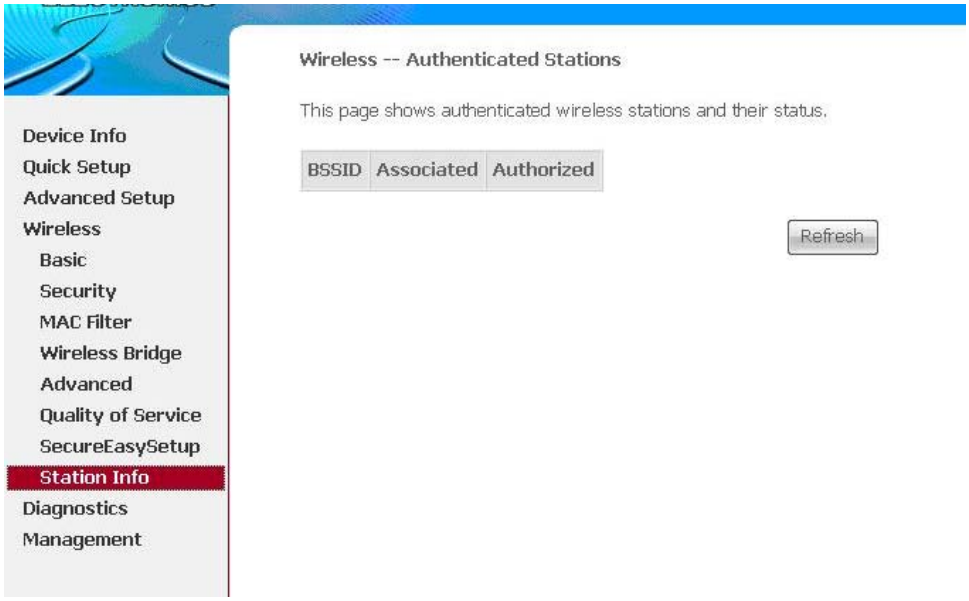


Figure 3.3.5: Wireless—Authenticated Stations

4.5.4 Configuration Example

4.5.4.1 How to connect STA to AP

This section will give a simple configuration example, it familiarize you with wireless configuration, and how to connect a wireless pc to the network. The topology below will be used:

Figure 25 Topology for STA connect to AP

4.5.4.1.1 Configuring wireless connection

1、Open the wireless-basic web page, the LAN Wireless Access Point Properties' screen appears(see figure26):

2、Check the Enable Wireless boxes

3、Change the default SSID to john_smith, make it be unique name. After setting, the web page appears (see figure 26)

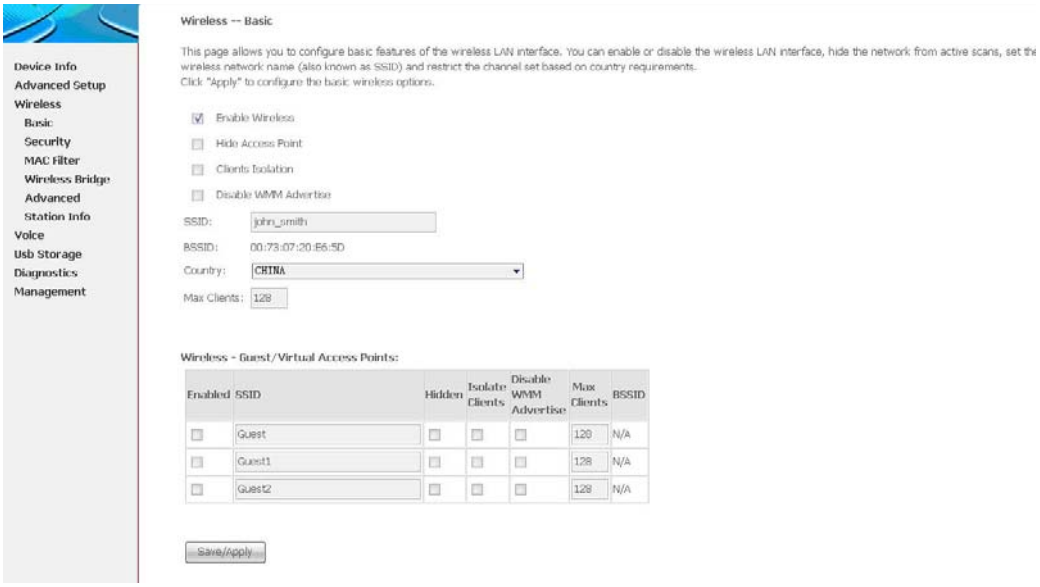


Figure 3.3.6: Wireless—Basic property setting

4、Click the Save/Apply button to save the setting.

4.5.4.1.2 Configuring a Wireless Windows XP Client

If your PC has wireless capabilities,Windows XP will automatically recognize this and create a wireless connection for you. You can view this connection under Window's Network Connections.

1. Open your Network Connections window from Window's Control Panel.

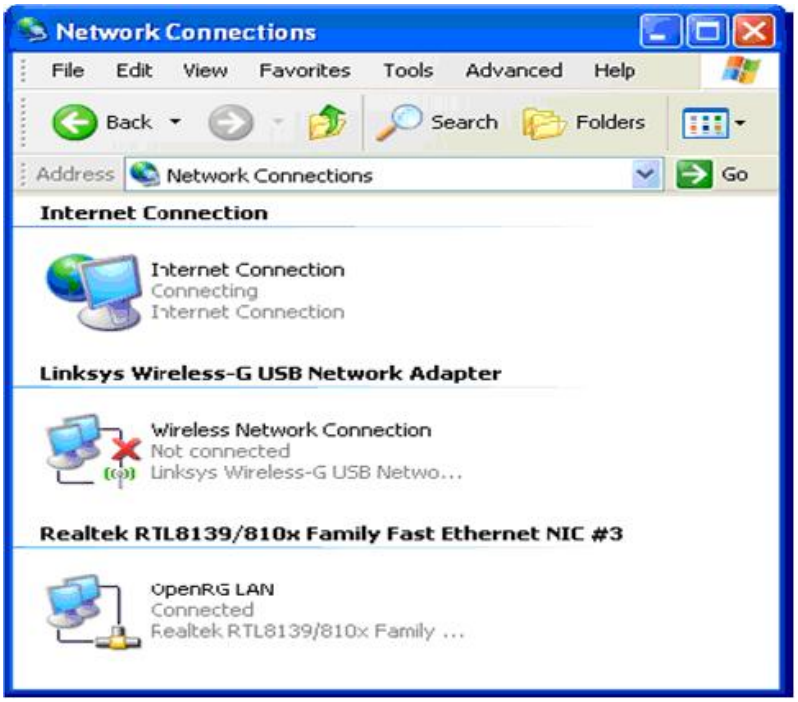


Figure 27 Network Connection

2. Double-click the wireless connection icon. The 'Wireless Network Connection' screen will appear, displaying all available wireless networks in your vicinity. If your gateway is connected and active, you will see wireless connection. Note that the connection's status is 'Not connected' and denned as .Unsecured wireless network..

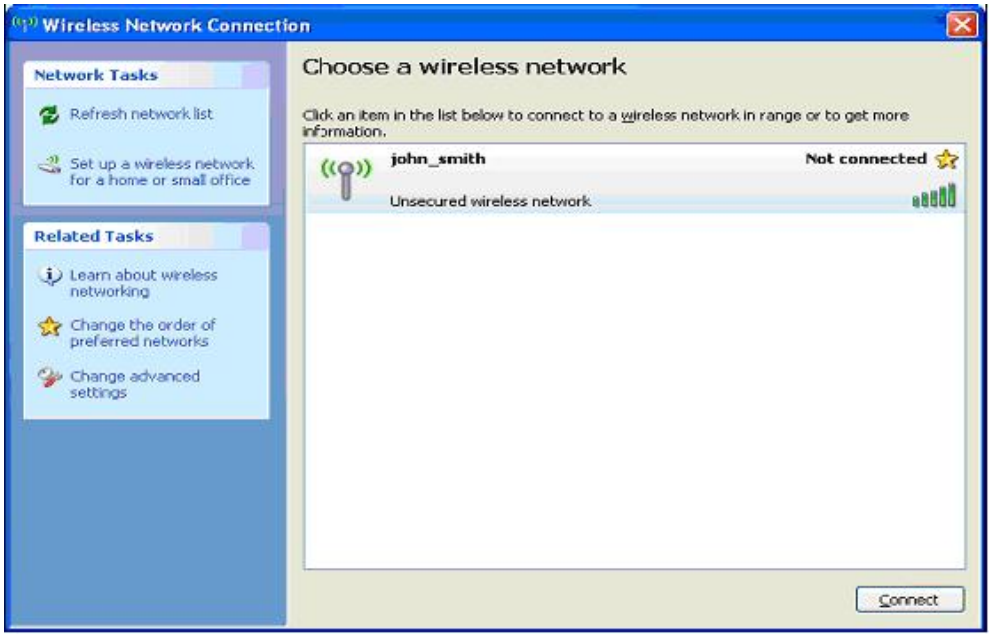
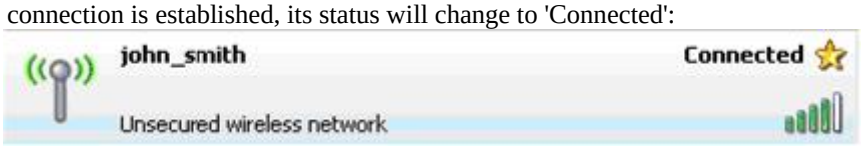

Wireless Network Connection
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Choose a wireless network
Click an item in the list below to connect to a wireless network in range or to get more information.
john_smith
Not connected
Unsecured wireless network
Connect

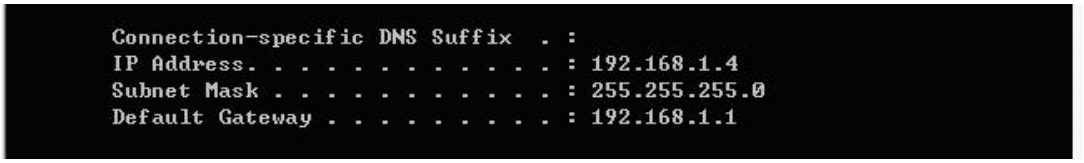
Figure 28 Wireless Connection

3. Click the connection once to mark it and then press the 'Connect' button at the bottom of the screen. After the connection is established, its status will change to 'Connected':



An icon will appear in the notification area, announcing the successful initiation of the wireless connection.

4. Once the client connects to the access point, it will get a ip address by dhcp protocol.see Figure below:



4.6 Voice (available)

4.6.1 Overview

DSL ROUTER's Voice over IP (VoIP) solution allows you to connect two or more parties over a single broadband connection, providing the benefits and quality of digital voice and other advanced features. These parties include IP phone, analog phone attached an ATA (Analog Telephone Adapter), and telephone on PSTN network. With a PBX (Private Branch eXchange) or a signaling gateway, you can even connect to VoIP phones armed with other protocols than SIP. DSL ROUTER enables you to place and receive calls over the Internet using a standard telephone set connected to SIP Proxy or other devices which have/include the same functions as SIP Proxy.
With proper dial-plan setting, calls on DSL ROUTER may be routed to PSTN network or VoIP network, depending on what digits you dial.

DSL ROUTER provides 2 FXS interfaces and 1 FXO interface. FXO is connected to telephone line, through which you dial up to Internet. Normally the telephone line is multiplexed with both telephone signal and data signal. If not filtered out by a splitter before entering FXO interface, the incoming PSTN calls will be routed to FXS-connected analog phone or other VoIP user. You can use up to 2 analog phones, each connected to one FXS interface. The two are called endpoint, and act as a independent role as IP phones. To configure VoIP account for each endpoint, please refer to 'SIP Basic Setting' page.

In order to use the DSL ROUTER's VoIP function, the first thing to do is to add some parameters through web pages that DSL ROUTER provides. Chapter 1.1 gives the overview of DSL ROUTER VOIP solution. Chapter 1.2 introduces the web page configuration, including SIP Basic Setting and SIP Advanced Setting. Chapter 1.3 shows how to manipulate/use DSL ROUTER's call function (such as redial), response function (such as call forward, call waiting), and so on. Chapter1.4 shows you some configuration examples, so let you use DSL ROUTER's VoIP function quickly and easily.

4.6.1.1 SIP Entities

DSL ROUTER's VoIP solution use SIP (Session Initiation Protocol) to create, modify, terminate calls. SIP is an "Internet" application-layer protocol that runs in User Agent and Server Systems for controling multimedia sessions between users, who may move from one location to another, and use terminal devices with various media capabilities. For more details about SIP, please see RFC3261.

In order to form concepts of SIP, terminology of SIP is displayed blow, and chart 1.1 shows their application.

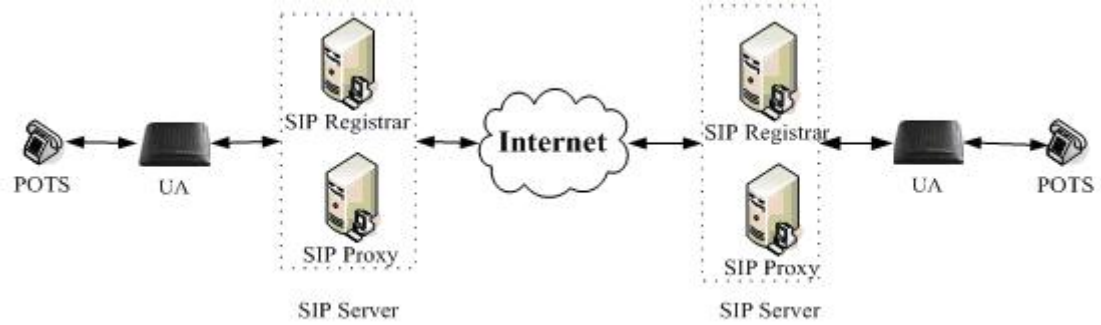
POTS: Plain old telephone service. The traditional telephones we use in home are POTS.

User Agent (UA): It includes UA Client (UAC), UA Server (UAS). UAC originates calls, and UAS listens for incoming calls. DSL ROUTER can server as UAS and UAC.

SIP Proxy: routes call requests. If we create a call to invite our friends or relatives through SIP, our call is routed through SIP Proxy, for only it knows your friends' or relatives' POTS's position.

SIP Registrar: maintains mappings from names (user ID) to addresses. How can an invite call identify you from so many users who use SIP to communication? The secrete is your user ID, which you have registered on the SIP Registrar. SIP Proxy uses user ID routes the coming call to your POTS.

NOTE: SIP Server has SIP Proxy's and SIP Registrar's function usually.



4.6.1.2 SIP Call Flows

4.6.1.2.1 Registration

SIP user agent sends a REGISTER message to registrar server, containing its SIP URL and location. Registrar server stores the binding of the two in its database, named location database. When other request provides a SIP URL and queries this database for the corresponding location, location database server will respond with the IP address.

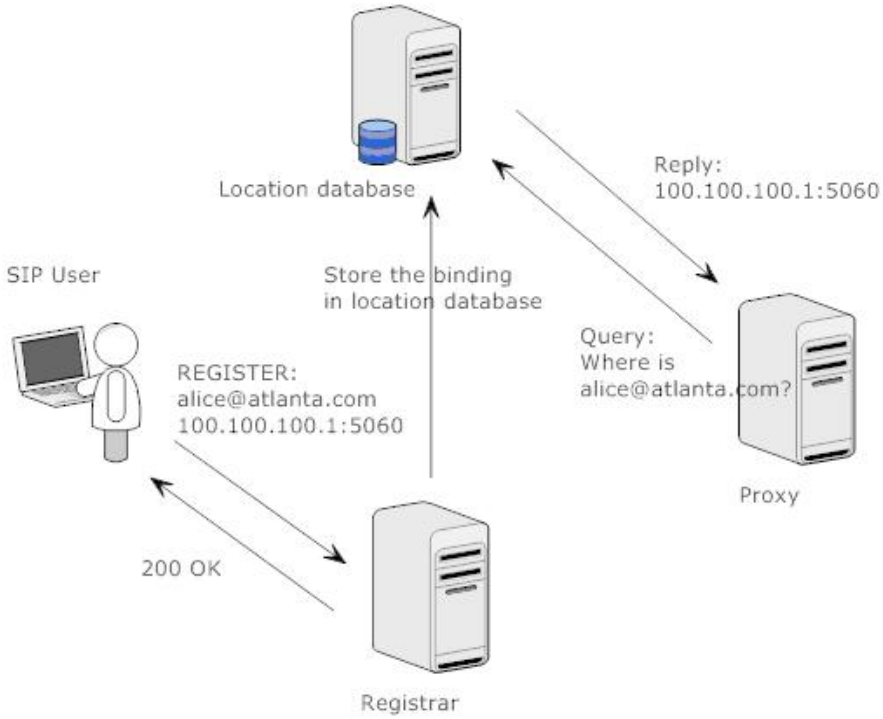


Figure1. Registration

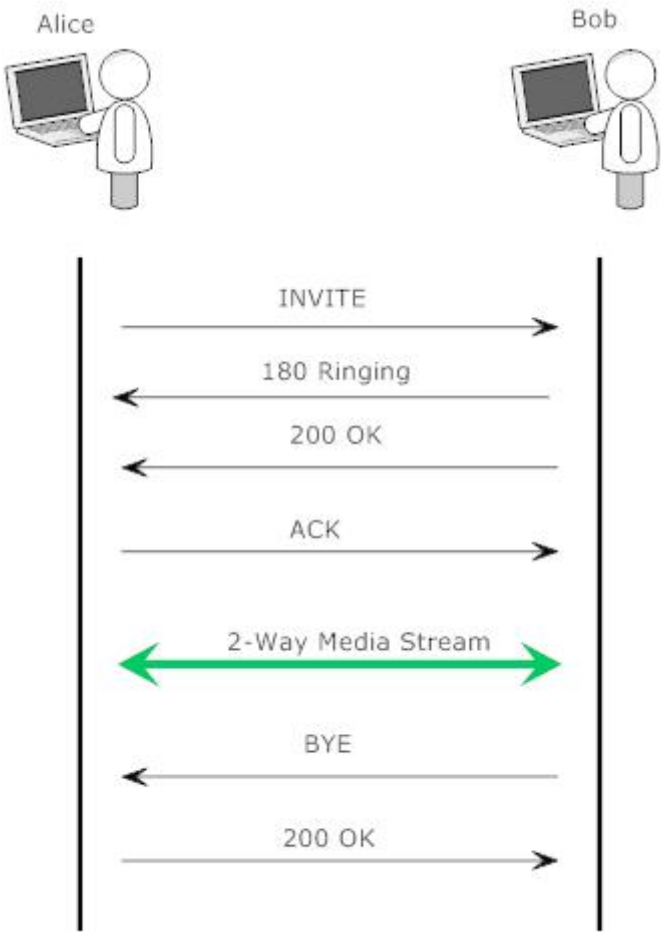
4.6.1.2.2 Simple Call Flow

Sometimes SIP user agents know the exact location of each other, and they are configured without proxy. In this case, both can talk directly.

Alice seizes here phone, keys in Bob's number, in SIP URL format. Assuming Bob is using a SIP-enabled IP phone with IP address 100.100.100.1, Bob's SIP URL should be something like bob@100.100.100.1. After Alice presses 'DIAL' button on her phone, a SIP INVITE message is sent to Bob's IP phone directly. Once Bob's IP phone receives this message, it rings, and meanwhile replies with another SIP message to Alice, then Alice will hear a ring-back tone.

Bob knows a incoming call is available, and off-hook his phone. At this time a 2-way voice connection is created, and both party are able to hear and talk with each other.

In this example, Bob first on-hooks his phone, producing an ACK message sent back to Alice. The arrival of this message will terminate the voice connection, making Alice hear a busy tone on her side.

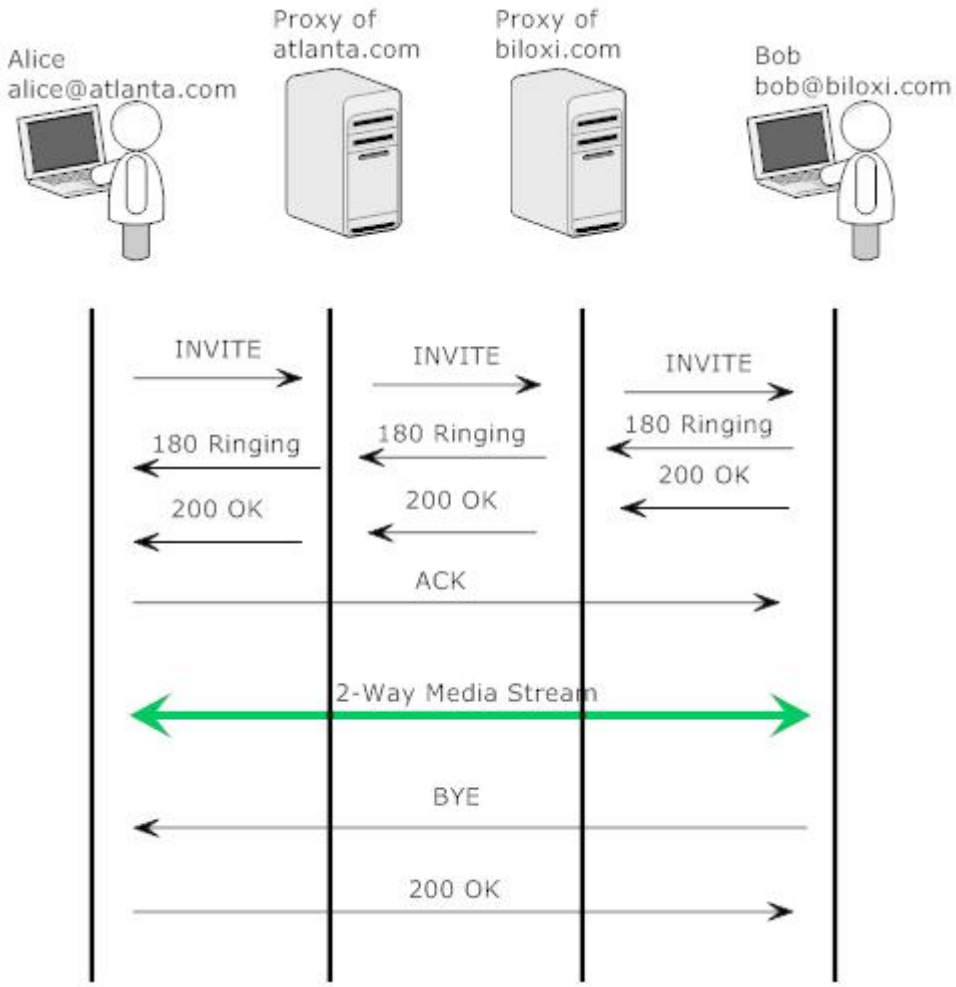


4.6.1.2.3 Call Flow in Proxy Mode

In proxy mode, every user agent takes use of proxy to relay its SIP message. Proxy may query a location database server about a SIP URL. Depending on the result, it may relay the request to a next-hop proxy, or send it to the destination peer.

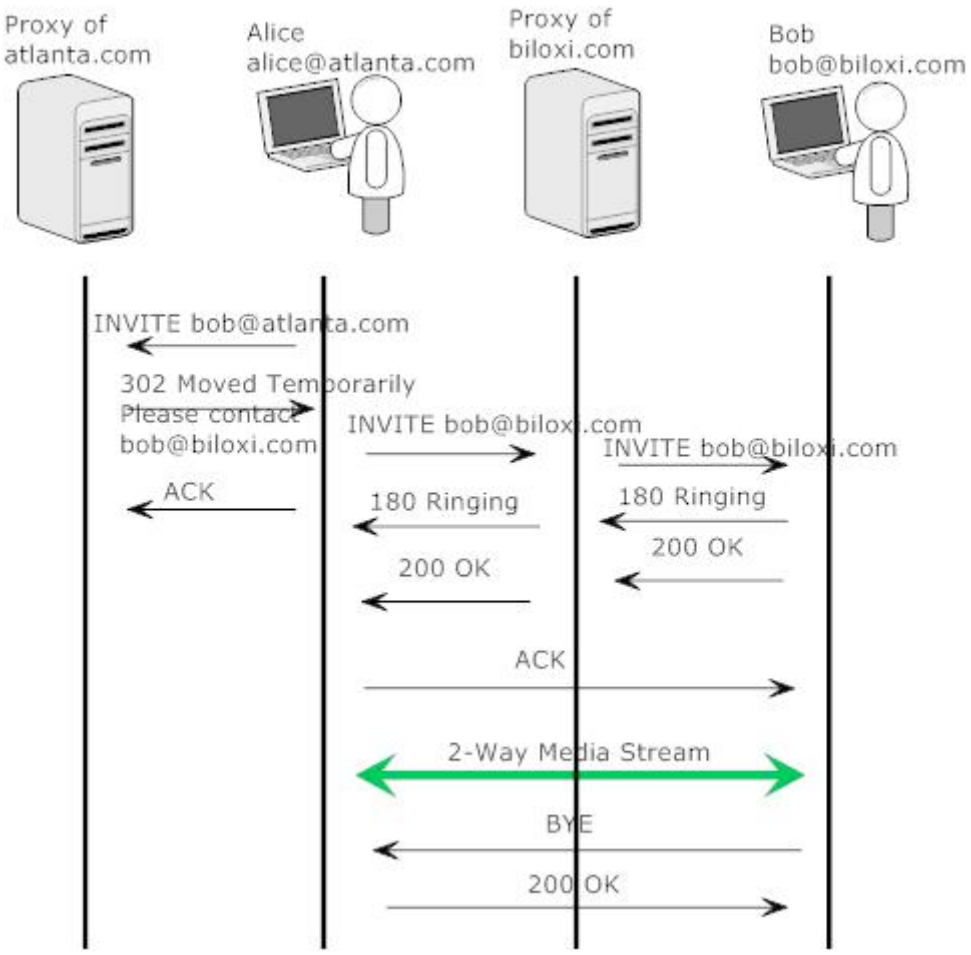
In this flow, Alice is located in atlanta.com. She is going to place a call to Bob, whose SIP URL is bob@biloxi.com. Alice's user agent passes the INVITE message to its proxy, atlanta.com. From the request URL in SIP message, Alice's proxy determines the next hop is proxy biloxi.com, and passes this message to it.

Finally bob's phone rings, also this triggers a message passed back to Alice's user agent, producing a ring-back tone in Alice's phone. Once Bob hooks up his phone, a 2-way voice stream is created.



4.6.1.2.4 Call Flow in Redirect Mode

In this flow Alice calls Bob at bob@atlanta.com. Alice's user agent sends the SIP message to its proxy, but gets a 302 message, indicating Bob now is resided in another location. Also this response also guides Alice how to reach its new location, bob@biloxi.com. This time Alice knows the correct location of Bob, and the call flow is like the ones in previous section.



4.6.2 Web Page Introduction

Once you have logged in web page, navigate to VoIP page from left menu tree. Here you can set some parameters you need to register SIP endpoints, place a call or some advanced feature. The VoIP page doesn't contains a 'Save' or 'Apply' button, but you can save your settings permanently by clicking 'Stop SIP client' or 'Start SIP client'.

4.6.2.1 SIP Basic Setting

Access the SIP Basic setting by clicking the 'SIP Basic Setting' tab under the 'Voice' menu. The SIP Basic Setting screen appears, it shows as figure 1.2.

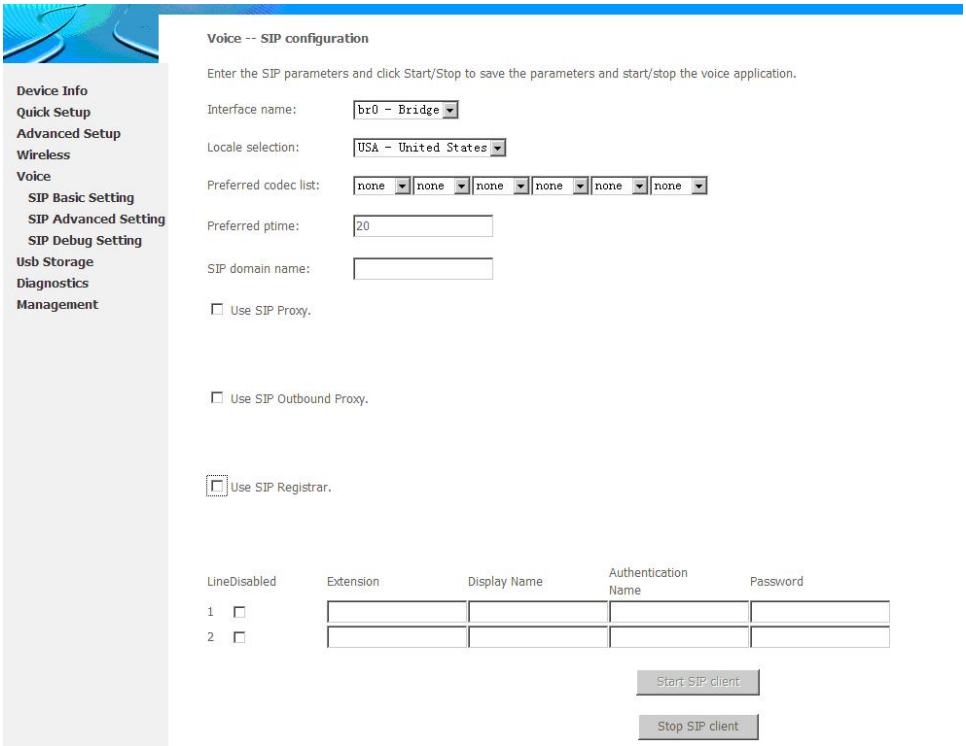


Figure 3.3.7: SIP Basic Setting Web Page

"SIP Basic Setting" web page enable you to set some parameters, such as Preferred codec list, Preferred ptime, SIP domain name and so on. The followings will show you how to configure the SIP Basic Setting Web Page step by step.

4.6.2.1.1 Interface name

Figure 3.3.8: Interface Name

This item provides for you to choose the way which DSL ROUTER's VoIP connect to SIP Proxy. There are two ways: br0-Bridge, PPPOE. If you do not configure the 'Wan' tab under the 'Advanced Setup' menu, there is only br0-Bridge you can choose. Default value is br0-Bridge. The method which you would like choose, please consult your Internet Service Provider (ISP).

4.6.2.1.2 Locale selection

Figure 3.3.9: Locale selection

This item provides for you to choose country where your locale in. The different country use different standards used by DSL ROUTER VoIP module, such as ring tone standard. Locale selection default value is USA..

4.6.2.1.3 Preferred code list

Figure 3.3.10: Preferred codec list

This item provides for you to specify the priority of codec, and the priority of codec declined from left to right.

Codecs define the method of relaying voice data. Different codecs have different characteristics, such as data compression and voice quality. For Example, G.723 is a codec that uses compression, so it is good for use where bandwidth is limited but its voice quality is not as good compared to other codecs such as the G.711.
If you specify none of the codecs, using the default value showed as figure 1.5, the DSL ROUTER will choose the codec automatically.

4.6.2.1.4 Preferred ptime

Figure 3.4.1: Preferred ptime

This item provides for you to set the Packetization Time (PT). The PT is the length of the digital voice segment that each packet holds. The default is 20 millisecond packets. If selecting 10 millisecond packets enhances the voice quality, as less information is lost due to packet loss, but doubles the load on the network traffic.

4.6.2.1.5 SIP domain name

Figure 3.4.2:SIP domain name

Fill in the SIP domain name or SIP server's IP address. If set to domain name, make sure it must be resolvable to SIP server's IP address.

4.6.2.1.6 Use SIP Proxy

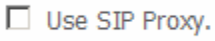


Figure 3.4.3: Use SIP Proxy

Select the check box if you DSL ROUTER uses a SIP proxy. SIP Proxy allows other parties to call DSL ROUTER through it. When this item is checked, the following fields appear:

Figure 3.4.4:SIP Proxy Parameters

SIP Proxy: Specify the proxy's IP address.
SIP Proxy port: The port that this proxy is listening on. Default port value is 5060.

4.6.2.1.7 Use SIP Outbound Proxy

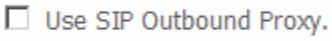


Figure 3.4.5: Use SIP Outbound Proxy

Some network service providers require the use of an outbound proxy. This is an additional proxy, through which all outgoing calls are directed. In some cases, the outbound proxy is placed alongside the firewall and is the only way to let SIP traffic pass from the internal network to the Internet. When this item is checked, the following fields become visible:

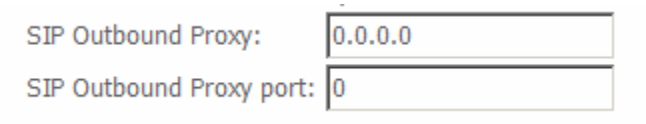


Figure 3.4.6: SIP Outbound Proxy parameters

SIP Outbound Proxy: The Outbound Proxy's IP address
SIP Outbound Proxy port: The port that the Outbound Proxy is listening on.
Both of them default value are as showed in figure 2.1.

4.6.2.1.8 Use SIP Registrar

Figure 3.4.7:Use SIP Registrar

Select this option to register with the proxy. You can register your USER ID on the SIP Registrar. SIP Registrar works with SP Proxy, allowing other parties to call DSL ROUTER through it. When this item is checked, the following field becomes visible:

Figure 3.4.8: Use SIP Registrar Parameters

SIP Registrar: The SIP Registrar's IP address.
SIP Registrar port: The port that SIP Registrar is listening on. Default value is 5060.

4.6.2.1.9 Line Settings

Figure 3.4.9: Line Settings

There are five options you can checked or filled in:
Line Disabled: Line number is a telephone port in DSL ROUTER to which you can connect a standard (POTS) telephone. If you checked this option, and the line corresponding you checked will be disable. You can not use it to initiate or accept any call.
Extension: This is telephone's VoIP user ID, used for identification to initiate and accept calls.
Display Name: A free text description which will be displayed to remote parties as your caller ID.
Authentication Name: The login name used for authentication with the SIP proxy.
Password: The password used for authentication with the SIP proxy.
NOTE: if you have entered/changed the parameters on the web site, you must click Start/Sop to save the parameters and Start/Stop the voice application.

4.6.2.2 SIP Advanced Setting

The advanced setting page contains those parameters that are not usually used. If you need advanced feature, such as FAX and MOH (Music on Hold), you can configure it here.

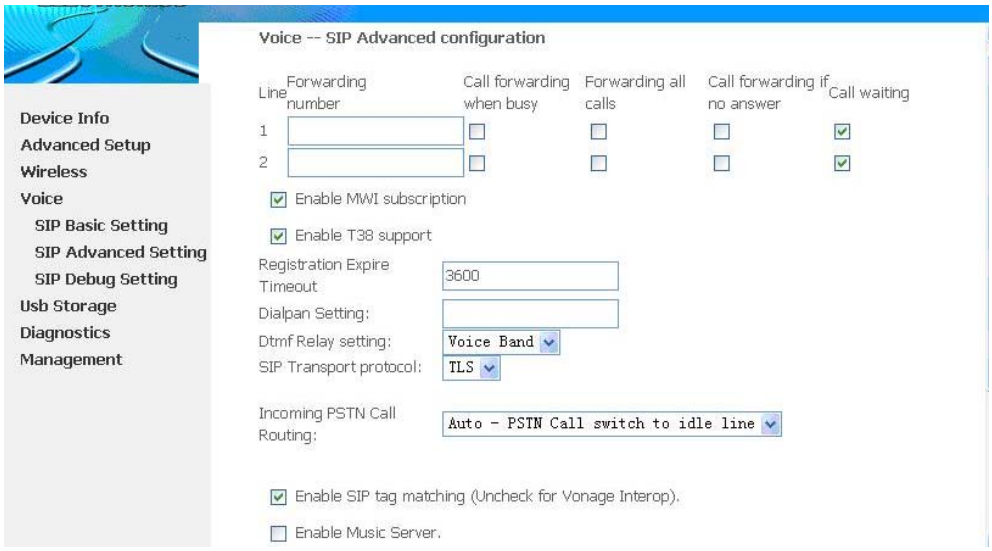


Figure CHP2.1 SIP Advanced Setting

4.6.2.2.1 Advanced Feature Setting

Figure 3.4.10:Advanced Feature Setting

- Forwarding number:

Set the number to forward a call. This number can also be set through dialing '*74<NUM>#' on the phone key pad. Refer to section 1.3.11 for more details.

- Call forwarding when busy

Enable 'Call forwarding when busy' feature. When this box is checked, incoming calls will be forwarded when the specific line is busy. It has the same effect as dialing '*72' on the phone pad.

- Forwarding all calls

Enable 'Call forwarding all' feature. When this box is checked, incoming calls will be forwarded unconditionally. Dialing '*73' can also accomplish this aim.

- Call forwarding if no answer

Enable 'Call forwarding no answer'. When this box is checked, incoming calls will be forwarded when it's not answered in 18s. Dialing '*71' also makes it.

- Call waiting

Enable 'Call waiting' feature on this line.

4.6.2.2.2 Enable MWI subscription

MWI stands for Message Waiting Indicator. When set this enabled, DSL ROUTER will send a SIP SUBSCRIBE message to proxy, asking for a notification when its voicemail status changes. When its status do changes, proxy will send a NOTIFY message to gateway, causing a MWI tone streamed to user's handset.

4.6.2.2.3 Enable T38 support

Checking this box will enable T38 support. When doing a fax transmission on DSL ROUTER, after fax tone been detected, fax transmission will switch to T38 mode.

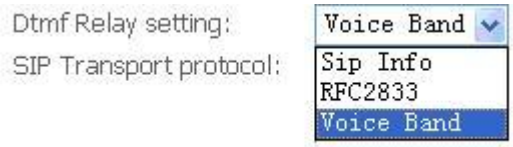
4.6.2.2.4 Registration Expire Timeout

It's the interval DSL ROUTER will initiate a new registration since last one. It's also known as 'registration assurance timer'. Gateway uses this mechanism to keep its binding record updated.

4.6.2.2.5 Dial Plan Setting

Set the VoIP dial plan. If user-dialed number matches it, the number will be processed by DSL ROUTER immediately.

4.6.2.2.6 Dtmf Relay setting



Set DTMF transmit method, which can be following values:

- SIP Info

Use SIP INFO message to transmit DTMF digits.

- RFC2833

Use RTP packet to encapsulate DTMF events, as specified in RFC 2833.

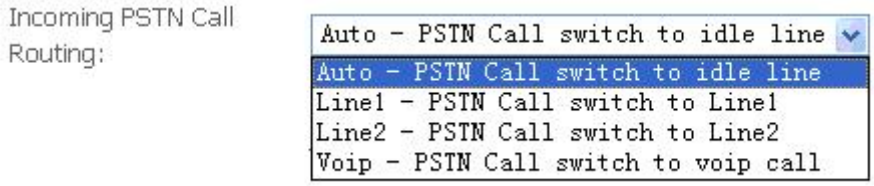
- Voice Band

DTMF events will be mixed with user voice in RTP packet.

4.6.2.2.7 SIP Transport protocol

Select the transport protocol to use for SIP signaling. Note SIP proxy and registrar need to support the protocol you choose.

4.6.2.2.8 Incoming PSTN Call Routing


Incoming PSTN Call Routing:
Auto - PSTN Call switch to idle line
Auto - PSTN Call switch to idle line
Line1 - PSTN Call switch to Line1
Line2 - PSTN Call switch to Line2
Voip - PSTN Call switch to voip call

Select the way incoming PSTN calls to be routed. It has following items:

- Auto - PSTN Call switch to idle line

DSL ROUTER will automatically select the idle line for incoming PSTN call.

- Line1 - PSTN Call switch to Line1

PSTN call will be routed to line 1. If it's busy, PSTN call will fail.

- Line2 - PSTN Call switch to Line2

PSTN call will be routed to line 2.

- VoIP - PSTN Call switch to VoIP call

PSTN call will be routed to VoIP extension, which is filled in 'PSTN Call Routing Data'.

4.6.2.2.9 Enable SIP tag matching

Enable the checking of the 'to' tag in SIP message. Enabling this feature may impose more strict checking on SIP messages. If you place DSL ROUTER in a Vonage network, using the Vonage server, make sure to uncheck it.

4.6.2.2.10 Enable Music Server

When set enabled, the holding party will act like a coordinator, and trigger the music server to stream music to the hold party. This is done by sending an INVITE without SDP to music server, and acknowledging server's response with an ACK message containing the SDP of the hold party. Music server then streams music to hold party.
Fill 'Music server' area with server's IP address, and specify the port in 'Music server port'.

4.6.3 VoIP functionality

This section will guide you how to use the functionality of DSL ROUTER in more detail. Some features involve 2 or 3 parties. In that case, note that all 3 parties have to be successfully registered.

4.6.3.1 Registering.

Before using any VoIP functionality, DSL ROUTER has to register itself to a registrar. DSL ROUTER also has to be configured with a proxy, which relays VoIP signaling to next hop. In fact, many implementations integrate these two into one server, so in many case registrar and proxy refer to the same IP.

a. Select the right interface to use for registering, depending on where Proxy/Registrar

resides. If use WAN link, make sure it's already up.

b. Fill 'SIP domain name' with SIP proxy's IP address or domain name. Note if we use domain name, it must be resolvable to proxy's IP address.
c. Mark 'Use SIP Registrar' box, and fill below IP/Port field with the right value.
d. Fill the extension information: 'Extension', 'Display Name', 'Authentication Name' and 'Password'. 'Authentication Name' and 'Password' must be pre-configured in registrar database.
e. Click 'Stop SIP client' (if VoIP application has been started already), then 'Start SIP client' to make above settings take effect.
f. VoIP LED should light on, indicating SIP client is successfully registered.

4.6.3.2 Placing a call

This section depicts how to place a basic VoIP call.

a. Pick up the handset on the phone.
b. Now you hear the dial-tone. Dial the extension of remote party
c. To end the dialing, wait for digit-timeout or just press '#' immediately.
d. After remote party answers the call, you're in voice connection.

4.6.3.3 Anonymous call

Anonymous call won't send the caller ID to remote party. This is useful if you don't want others know whom you are.

a. Pick up the handset on the phone.
b. Dial '*83' to enable anonymous call.
c. Hook on the handset, and dial another extension as you like. Now your caller ID information is blocked.
d. To enable caller ID transmission again, dial '*84' on the key pad.

4.6.3.4 Do not disturb (DND)

If DND enabled, all incoming calls will be rejected. DND is useful if you don't want others to bother you.

a. Pick up the handset on the phone.
b. Dial '*86' to enable DND function
c. Hook on the phone. Now your phone will reject all incoming calls.
d. To disable DND, press '*87' on the key pad.

4.6.3.5 Redial.

For outgoing calls, DSL ROUTER will remember the number you dial. Next time when you want to dial that person, DSL ROUTER provide you the redial functionality.

a. To re-dial the latest dialed person, press '*68' on the key pad.
b. Now you have made the call, as if you just dialed the whole number.

4.6.3.6 Call return.

For incoming calls, DSL ROUTER remembers the number of calling party.

a. To return a call, press '*69'
b. Now you have made the call as if you have dialed the whole number

4.6.3.7 Call hold

Call hold enable you put a call to a pending state, and pick it in future.

a. Assuming you are in a voice connection, you can press ‘FLASH’ to hold current call.
b. Now you can call another party, or press ‘FLASH’ again to return to first call.

4.6.3.8 Call waiting.

Enabling call waiting will allow third party to call in when you’re in a voice connection.

a. Pick up the phone attached to DSL ROUTER.
b. Press ‘*61’ to enable call waiting function.
c. Assuming you’re in a voice connection, when another call comes in, DSL ROUTER will stream a call waiting tone to your phone, indicating another call is available.
d. Press ‘FLASH’ will switch to this call and the initial call will put to hold automatically.
e. Press ‘FLASH’ multi-times will switch between these two calls back and forth.
f. Pressing ‘*60’ will disable call waiting function.

4.6.3.9 Blind transfer

Bind transfer will transfer the current call to a third party blindly, regardless of whether the transfer is successfully or not.

a. Assume you have already been in a voice connection.
b. Press ‘FLASH’ to hold the first party.
c. Dial a third party.
d. Before the third party answers the call, hook on your phone.
e. Now the first party takes over the call and is in connection with the third party.

4.6.3.10 Consultative transfer

Consultative transfer will let the third party answer the transferred call, and then hook on the transferring party. It’ more gentle than blind transfer.

a. Assume you have already been in a voice connection with a first party.
b. Press ‘FLASH’ to hold the first party.
c. Dial a third party.
d. After the third party answers the call, hook on your phone.
e. Now the first party takes over the call and is in connection with the third party.

4.6.3.11 Call forwarding no answer

If this feature enabled, incoming calls will be forwarded to third party when you doesn’t answer them. It involves two steps: setting the forwarding number and enable the feature.

a. Dial ‘*74<NUM>#’ to set forwarding number, where ‘NUM’ is the number of the party whom the call is forwarded to.
b. Dial ‘*71’ to enable call forwarding no answer. That is, when our phone doesn’t answer incoming call, this call will be forwarded.
c. Press ‘*70’ will disable call forwarding no answer.

4.6.3.12 Call forwarding busy

If this feature enabled, incoming calls will be forwarded to third party when you busy. It involves two steps: setting the forwarding number and enable the feature.

a. Dial ‘*74<NUM>#’ to set forwarding number, where ‘NUM’ is the number of the party whom the call is forwarded to. Note if we have already set forwarding number before, this step can be omitted.
b. Press ‘*72’ to enable call forwarding busy. That is, when our phone gets busy, this call will be

forwarded.

c. Press ‘*70’ will disable call forwarding busy.

4.6.3.13 Call forwarding all

If this feature enabled, incoming calls will be forwarded to third party without any reason. It involves two steps: setting the forwarding number and enable the feature.

a. Dial ‘*74<NUM>#’ to set forwarding number, where ‘NUM’ is the number of the party whom the call is forwarded to. Note if we have already set forwarding number before, this step can be omitted.
b. Press ‘*73’ to enable call forwarding all. That is, all incoming alls will be forwarded to the third party.
c. Press ‘*75’ will disable call forwarding all, but let call forwarding no answer and call forwarding busy unchanged.
d. Press ‘*70’ will disable all call forwarding function.

4.6.3.14 3-Way conference

3-way conference enables you to invite a third party to a call, and every person in the conference is able to hear others’ voice.

a. Assume you are in connection with a first party.
b. Press ‘FALSH’ to put the first party on hold.
c. Dial a third party.
d. After the third party answers the call, press ‘FLASH’ again to invite the first party.
e. Now all three parties are in a 3-way conference.

4.6.3.15 T38 Faxing

To make T38 faxing, enable T38 support on the web. After that, connect a fax machine to a FXS port of DSL ROUTER. Now you can treat it as a normal phone and is able to send or receive fax to or from other fax machines on the VoIP network.

In initial setup, faxing behaves like a normal call. After DSL ROUTER detects the fax tone, it switch to T38 mode, and use it as the transmit approach.

4.6.3.16 Pass-through Faxing

If T38 support is not enabled, faxing will use normal voice codec as its coding approach. So this mode looks much like normal phone calls.

4.6.3.17 PSTN to VoIP call

For incoming PSTN call, DSL ROUTER can route it to local FXS-attached analog phones or other VoIP extension, depending on the setting. In ‘Voice/SIP Advanced Setting’, there are four schemes in ‘Incoming PSTN call routing’ drop list:

- Auto - PSTN Call switch to idle line

DSL ROUTER will automatically select the idle line for incoming PSTN call.

- Line1 - PSTN Call switch to Line1

PSTN call will be routed to line 1. If it’s busy, PSTN call will fail.

- Line2 - PSTN Call switch to Line2

PSTN call will be routed to line 2.

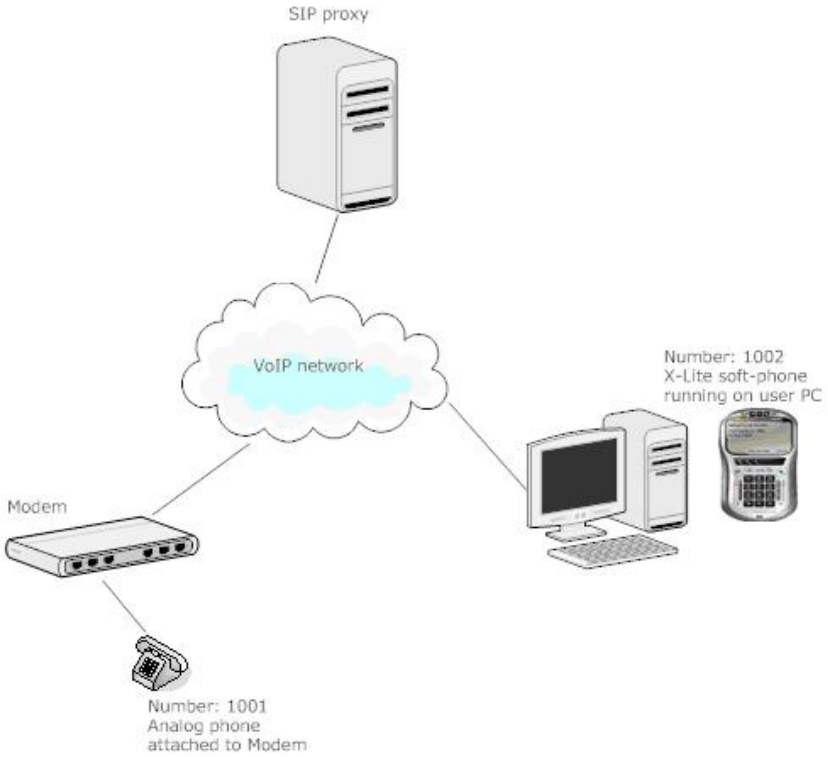
- VoIP - PSTN Call switch to VoIP call

PSTN call will be routed to VoIP extension, which is filled in ‘PSTN Call Routing Data’.

4.6.4 Configuration Example

4.6.4.1 VoIP Call

This section describes how to setup a basic VoIP call with DSL ROUTER. To make a 2-way call, we need the help of another party. Here we use X-Lite, which is downloadable on http://www.xten.com.
The overall diagram is shown below. Besides 2 peers (GWGW gateway and X-Lite soft-phone running on user PC), there should be a SIP server exists on Internet or local network in LAN side of DSL ROUTER, depending on interface selection on VoIP configuration page. In this example, we use Asterisk, which is available on http://www.asterisk.org.
Make sure both DSL ROUTER and soft-phone should be able to reach SIP server. A 'ping' command on DSL ROUTER console and user PC can achieve this.



4.6.4.1.1 Configure SIP server

In this example, Asterisk acts as a registrar and a proxy. It accepts registration from VoIP network, binding the peer's SIP URL with its location (such as IP address). For call request from various peers, Asterisk first checks if it's authorized. If not, it simply denies it. And for incoming calls requesting other extensions belonging to it, Asterisk will find the corresponding location, and relay the SIP message to it.
First make sure Asterisk is configured with user information. Note that some other SIP server don't need you to configure this in advance, so in that case simply skip this step.
Asterisk SIP configuration file is located in /etc/asterisk/sip.conf. A sample configuration is shown below, with brief semicolon-separated explanation in the right:

```
bindport=5060        ; service port
bindaddr=192.168.1.237        ; binding IP address

; other configuration line omitted here...
```

```
[1001]      ; extension
type=friend
secret=1001      ; password
host=dynamic
canreinvite=no
context=sip      ; you must configure corresponding context 'sip' in extensions.conf
```

This sample configuration file only contains the information for 1001. To add other extension, simply add similar section in SIP.conf.
Before rushing to next step, make sure Asterisk is running.

4.6.4.1.2 Configure DSL ROUTER SIP

DSL ROUTER's SIP configuration page is shown below. Domain, proxy and registrar must be set to Asterisk's IP, and they are the same. Extension and authentication credential must be the same as what you set in SIP server. After basic filling is complete, just press the buttons below to re-run SIP module to make these settings take effect.

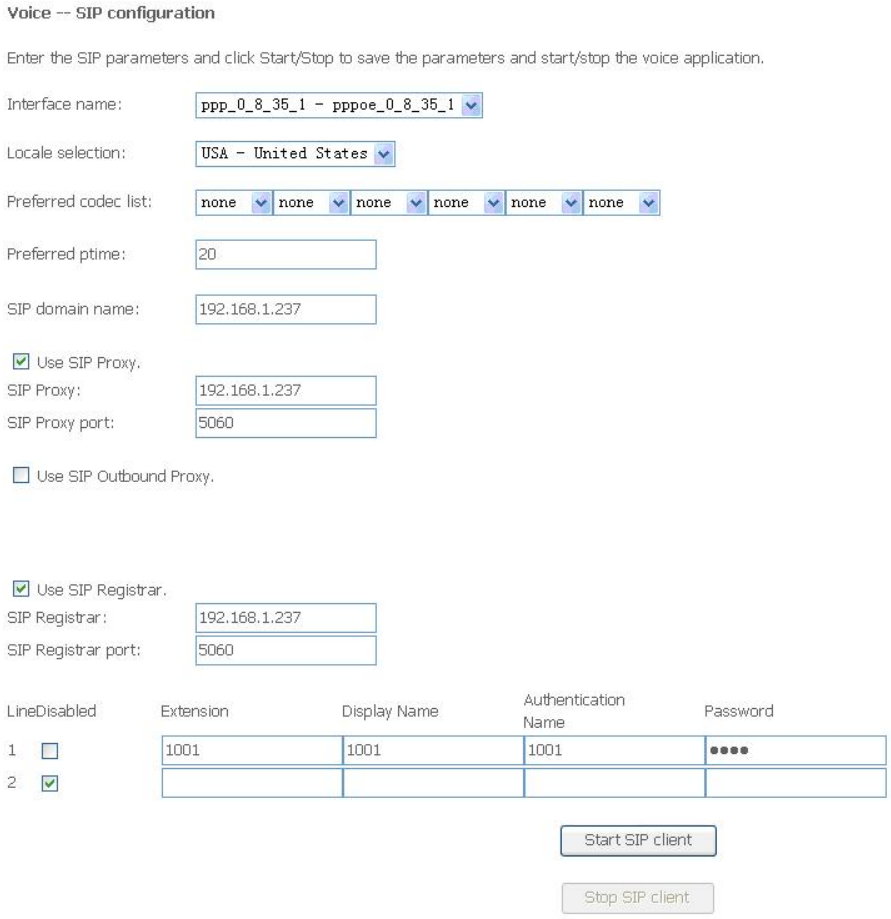


Figure 3.5.1: Voice SIP configuration

4.6.4.1.3 Configure the soft-phone

Soft-phone is configured with extension 1002. The configuration window is shown in below figure. After return to main window, a 'Logged in' message indicates the soft-phone is successfully registered.

Figure 3.5.2: Soft-phone configure

4.6.4.1.4 Test VoIP call

Seize the phone attached to DSL ROUTER, dial the number of soft-phone, 1002. Soft-phone should rings, with calling party's number information shown on it's LCD. Answer the call on soft-pone will create a 2-way VoIP calling. At this point, your VoIP call is successful.

4.6.4.2 PSTN-to-VoIP Call

With the function of the FXO interface on DSL ROUTER, PSTN calls to FXO number can be routed to FXS legs on the gateway, or to extensions on VoIP network. VoIP calls, if their numbers match PSTN dial-plan, will be routed to PSTN network too. However, in current implementation, we can't change PSTN dial-plan on the fly, so it's unable to call PSTN number freely.

In below figure, the telephone line connected to FXO interface is assigned with number 2001. In web page, PSTN calls are configured routed to VoIP extension 1002. So if a PSTN party 2002 calls 2001, this call will be forwarded to 1002.

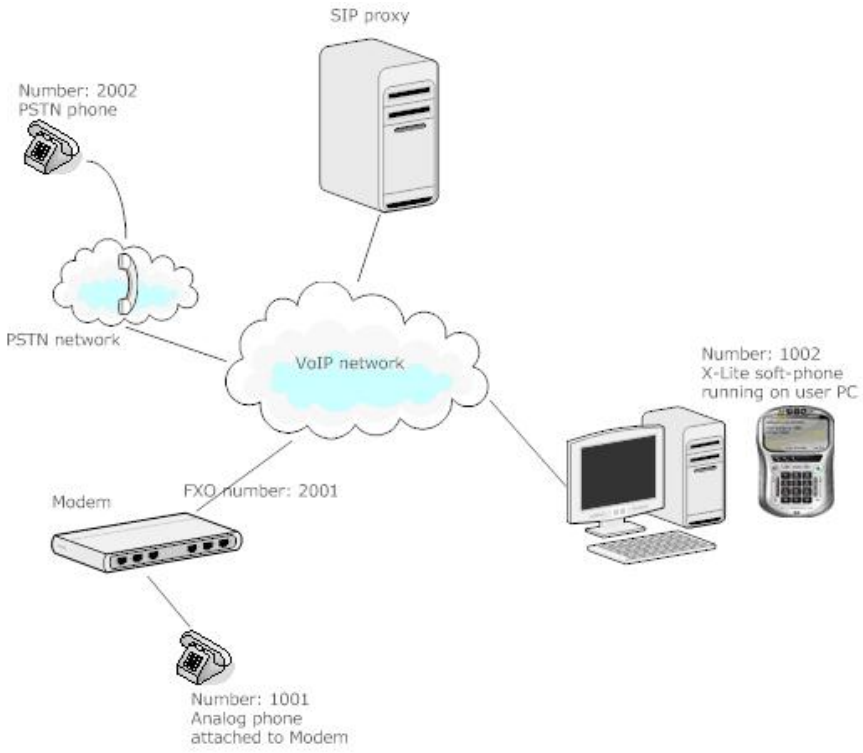


Figure 3.5.3:PSTN-to-VoIP Call topology

4.6.4.2.1 Configure DSL ROUTER SIP

In SIP configuration page, set PSTN call routing rule and route data as follows:

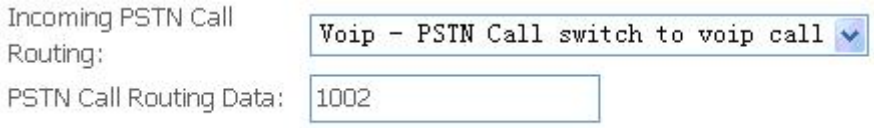


Figure 3.5.4:Configure DSL Router SIP

Stop and start SIP call client to make the change take effect.

4.6.4.2.2 Test PSTN-to-VoIP call

As the figured depicted, if PSTN user 2002 dials 2001, 1002 soft-phone will get the call.

4.7 Usb Storage

We Access the Usb Storage device on DSL router, We must use FTP Protocol to operate usb device, There are two functions in this chapter:

. FTP Server function :Lan side PC can logon to operate USB file

. FTP Client function :Can download file from internet to USB.

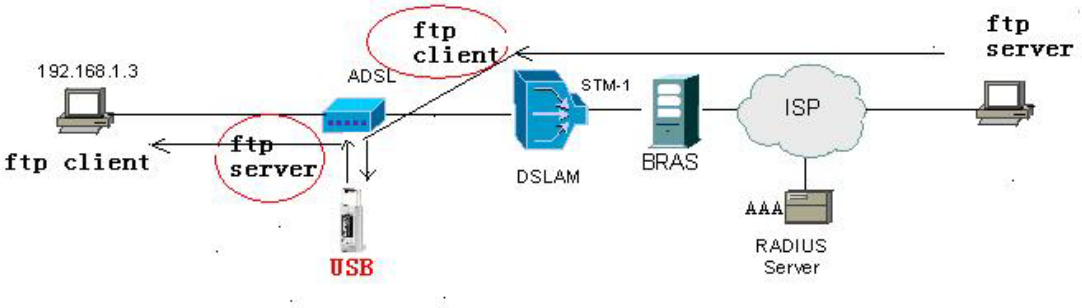


Figure 3.5.5: Usb Storage topology

4.7.1 FTP Server Configure

FTP: FTP (File Transfer Protocol) is a protocol for exchanging files on the Internet. The standard Internet protocol for downloading, or transferring, files from one computer to another. You can use this standard, for example, to offer files for downloading or to receive files from other users.

4.7.1.1 Setting Parameters and configure example

FTP Listening Port: The default FTP Listening Port is 21, here the user can modify the port value.
Max Connections for the same IP: It means the max connections the user going to set, note that 0 means no restrict. It connects automatically.
FTP Account Management: There are three levels account, ftpadmin account has the biggest authority, it can view, download and upload files. Ftpuser account can view and download files. anonymous account only has the view authority.

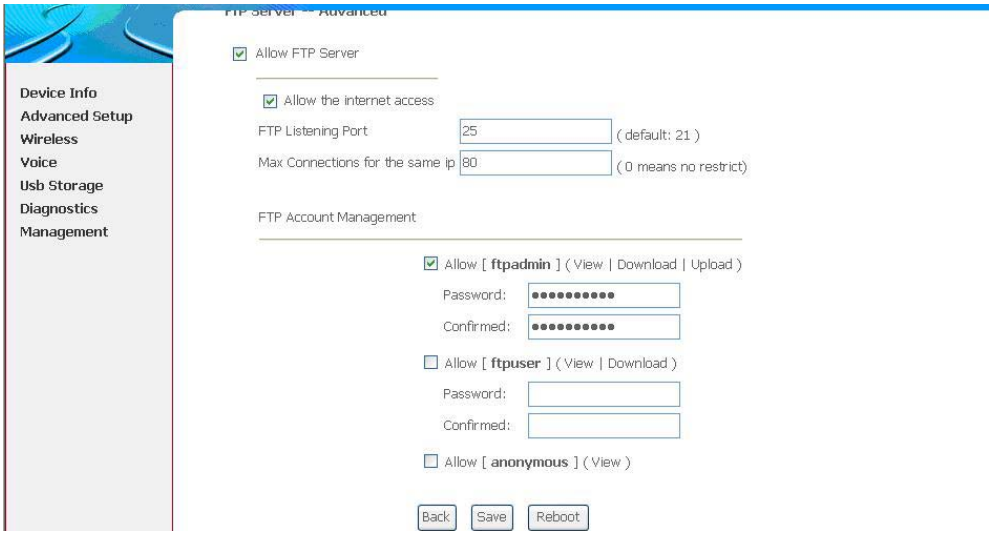


Figure 3.5.6:FTP Server Config

Note: After click “save” button, you need to reboot the modem to activate this setting.

4.7.1.2 Ftp client Setting

Local Path: When you insert USB storage, it will show the USB storage information to us, and you can select which storage to store.
Username: The account name which is setted in the FTP Server Configure WEB UI.
Password: The same with above.
Port: The same with above.
Remote URL: It is the remote FTP address where you are going to download files. When we download files, we store it to Local Path.

The following is the example how to configure the setting.

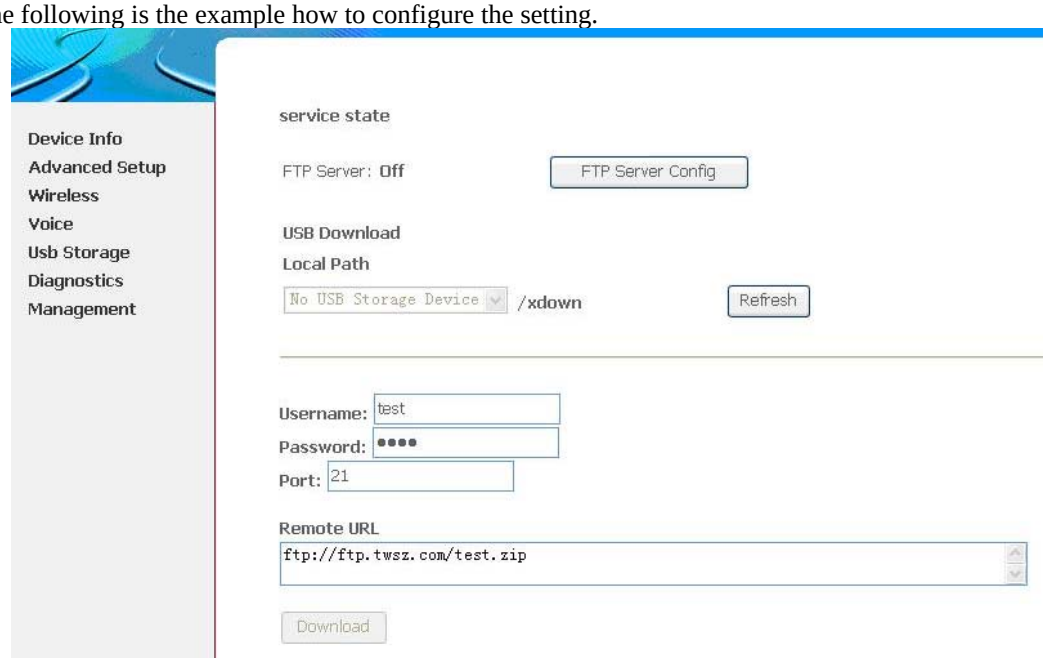


Figure 3.5.7:Ftp client Setting

4.8 Diagnostics

Click “Diagnostics” to show the interface.
Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

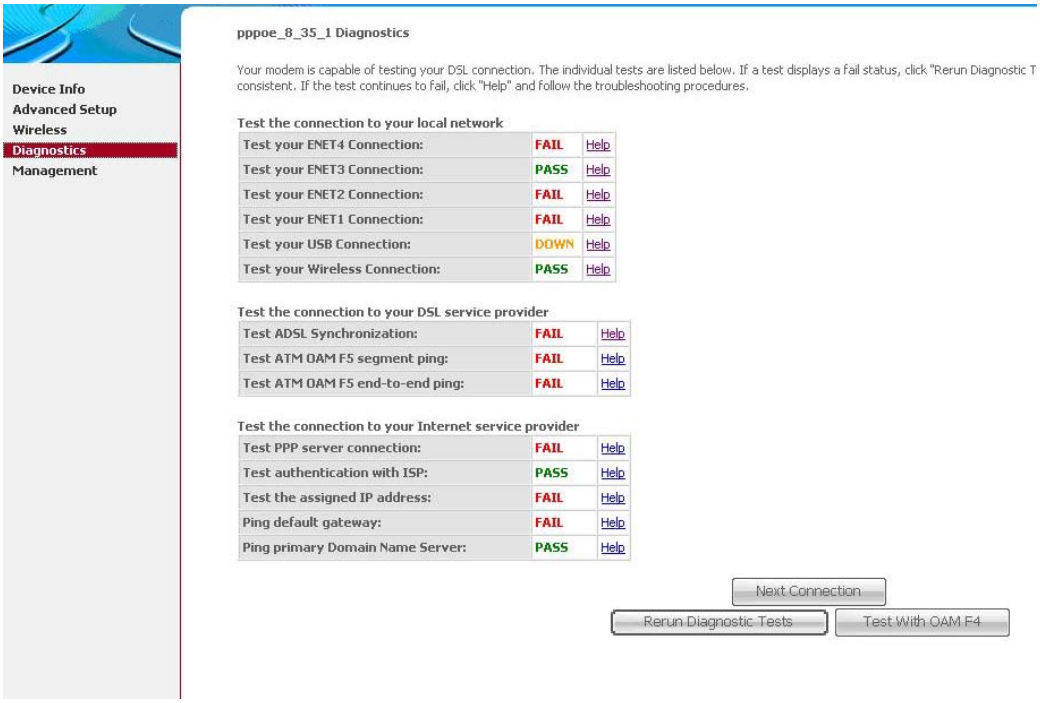

Device Info
Advanced Setup
Wireless
Diagnostics
Management
pppoe_8_35_1 Diagnostics
Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic T
consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.
Test the connection to your local network
Test your ENET4 Connection: FAIL Help
Test your ENET3 Connection: PASS Help
Test your ENET2 Connection: FAIL Help
Test your ENET1 Connection: FAIL Help
Test your USB Connection: DOWN Help
Test your Wireless Connection: PASS Help
Test the connection to your DSL service provider
Test ADSL Synchronization: FAIL Help
Test ATM OAM F5 segment ping: FAIL Help
Test ATM OAM F5 end-to-end ping: FAIL Help
Test the connection to your Internet service provider
Test PPP server connection: FAIL Help
Test authentication with ISP: PASS Help
Test the assigned IP address: FAIL Help
Ping default gateway: FAIL Help
Ping primary Domain Name Server: PASS Help
Next Connection
Rerun Diagnostic Tests
Test With OAM F4

Figure 3.5.8: Diagnostics page

4.9 Management

4.9.1 Settings

4.9.1.1 Settings Backup

Click the “Backup Settings”, backup the DSL router configurations.

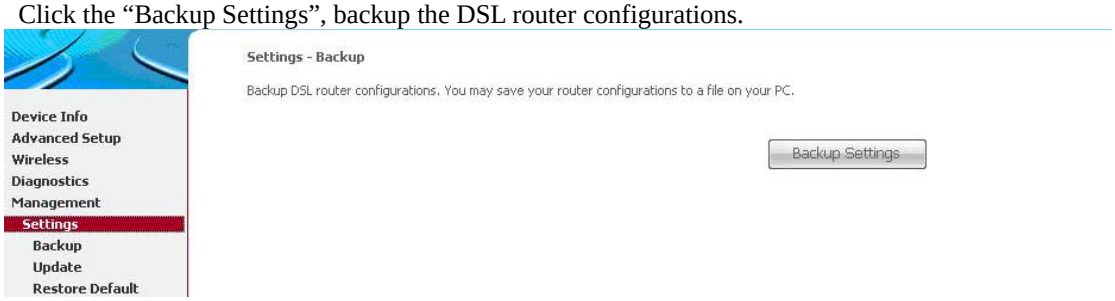


Figure 3.5.9:Backup Config

4.9.1.2 Settings Update

Click the “Browsing...” button, select the correct update configure settings file. Then click the “Update Settings” to update the Modem settings.

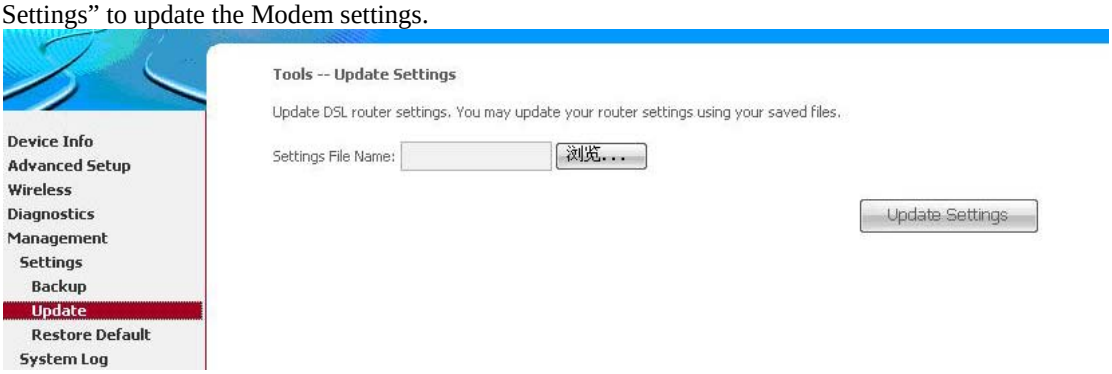


Figure 3.5.10: Update Settings

4.9.1.3 Settings Restore Default

Click “Restore Default Settings” to restore DSL router settings to the factory defaults.

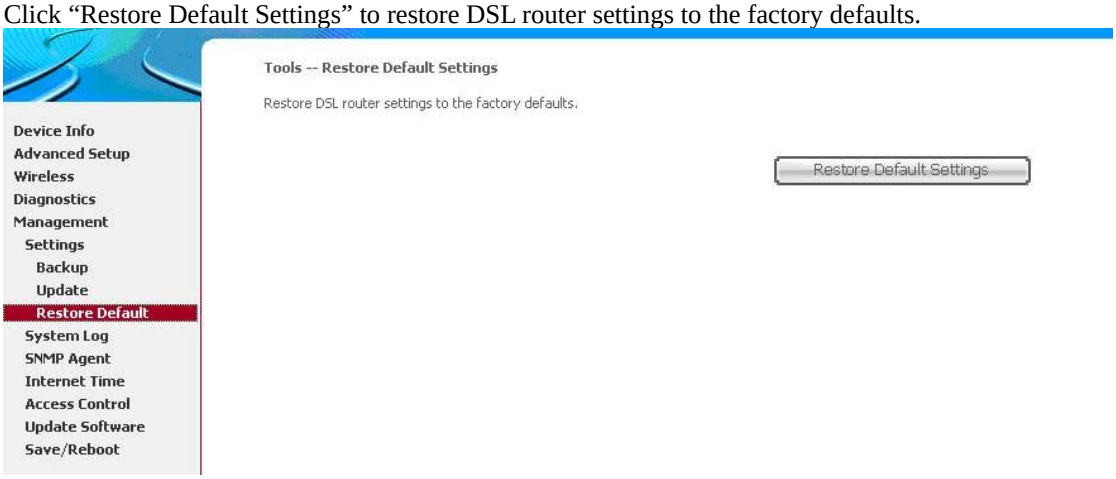


Figure 3.6.1: Restore Default Settings

4.9.2 System Log

Click “System Log” to show the following interface. The system log dialog allows you to view the system log and configure the system log options.

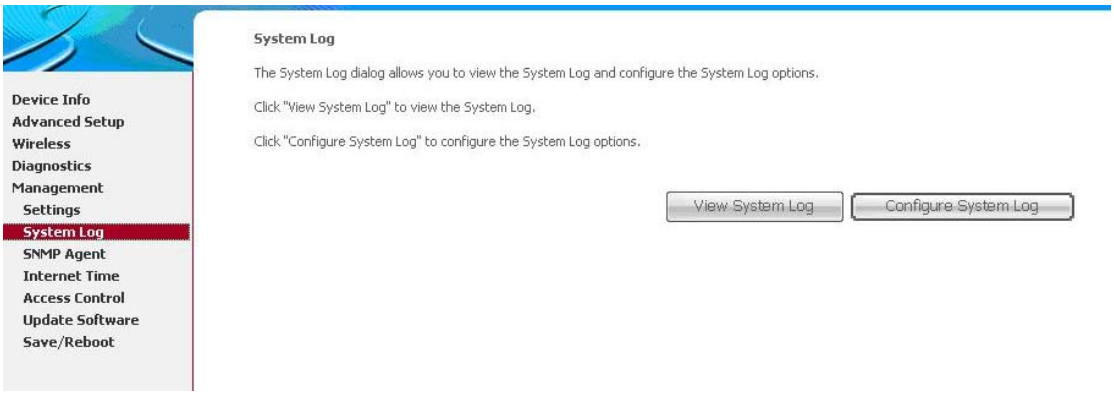
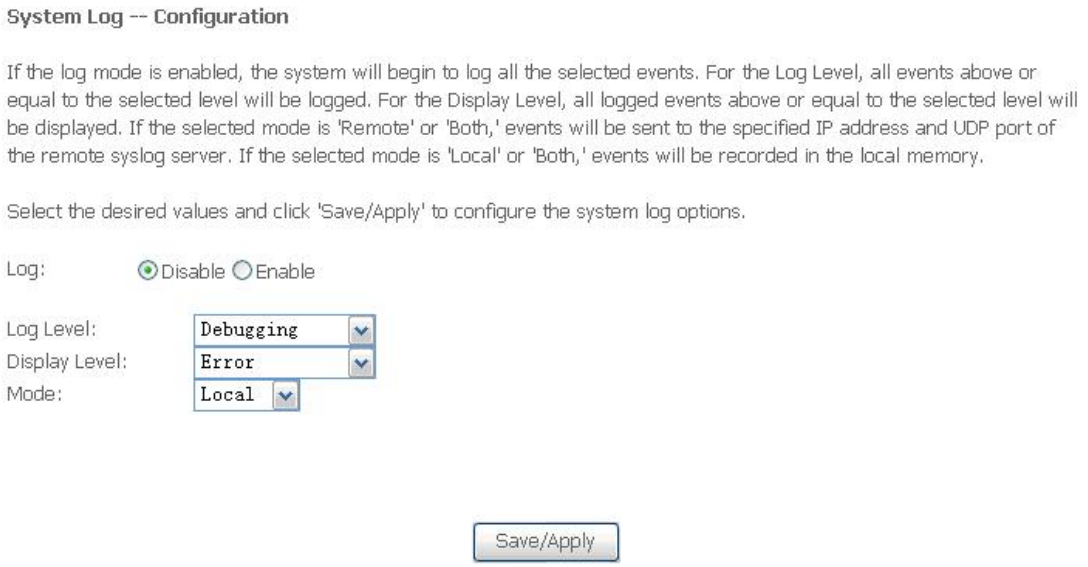


Figure 3.6.2: System Log overview

Click “Configure System Log” to show the following interface. You can enable or disable the system log and then select the log level, display level and mode, and click “Apply” to end your configurations.


System Log -- Configuration
If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.
Select the desired values and click 'Save/Apply' to configure the system log options.
Log: Disable Enable
Log Level: Debugging
Display Level: Error
Mode: Local
Save/Apply

Both the log level and display level have eight choices. The default log level is “Debugging” and the default display level is “Error”.

The mode options are “Local”, “Remote”, and “Both”. The default one is “Local”.

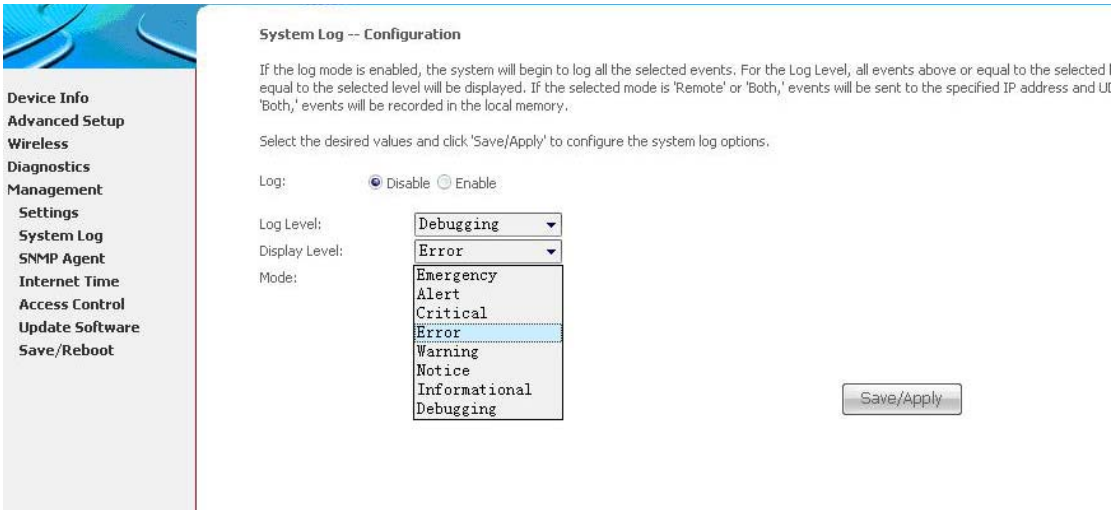

System Log -- Configuration
If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected l
equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UI
'Both,' events will be recorded in the local memory.
Select the desired values and click 'Save/Apply' to configure the system log options.
Log: Disable Enable
Log Level: Debugging
Display Level: Error
Mode:
Emergency
Alert
Critical
Error
Warning
Notice
Informational
Debugging
Save/Apply
Device Info
Advanced Setup
Wireless
Diagnostics
Management
Settings
System Log
SNMP Agent
Internet Time
Access Control
Update Software
Save/Reboot

Figure 3.6.3: System Log Config1

If you select “Remote” or “Both”, all events will be transmitted to the specified UDP port of the

specified log server.

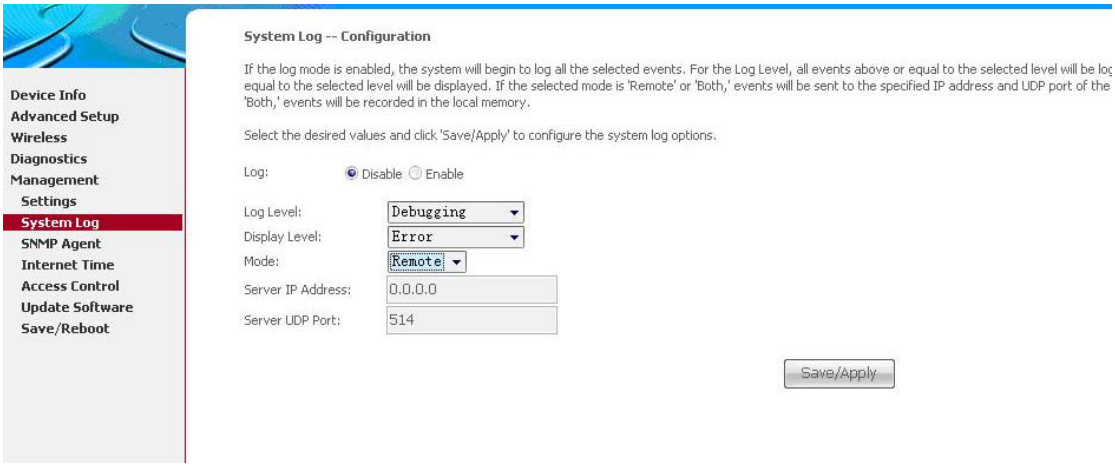

Device Info
Advanced Setup
Wireless
Diagnostics
Management
Settings
System Log
SNMP Agent
Internet Time
Access Control
Update Software
Save/Reboot
System Log -- Configuration
If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be log
equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the
'Both,' events will be recorded in the local memory.
Select the desired values and click 'Save/Apply' to configure the system log options.
Log:
Disable
Enable
Log Level:
Debugging
Display Level:
Error
Mode:
Remote
Server IP Address:
0.0.0.0
Server UDP Port:
514
Save/Apply

Figure 3.6.4: System Log Config2

After operations under “Configure System Log”, click “View System Log” to query the system logs. In this example, the “View System Log” is a system default one.

Note: The log and display of the system events are above the set level. If you intend to record all information, you need to set the levels as “Debugging”.

System Log

Date/Time	Facility	Severity	Message
Jan 1 01:38:08	user	crit	kernel: ADSL G.994 training
Jan 1 01:38:16	user	crit	kernel: ADSL G.992 started
Jan 1 01:38:20	user	crit	kernel: ADSL G.992 channel analysis
Jan 1 01:38:24	user	crit	kernel: ADSL G.992 message exchange
Jan 1 01:38:25	user	crit	kernel: ADSL link up, interleaved, us=1146, ds=25505
Jan 1 01:38:26	daemon	crit	pppd[628]: PPP server detected.
Jan 1 01:38:26	daemon	crit	pppd[628]: PPP session established.
Jan 1 01:38:27	daemon	err	pppd[628]: Couldn't increase MRU to 1500
Jan 1 01:38:27	daemon	err	pppd[628]: Couldn't increase MRU to 1500
Jan 1 01:38:27	daemon	crit	pppd[628]: PPP LCP UP.
Jan 1 01:38:27	daemon	crit	pppd[628]: Received valid IP address from server. Connection UP.
Jan 1 01:38:33	daemon	err	user: tr69c: Unable to retrieve attributes in scratch PAD
Jan 1 01:38:33	daemon	err	user: Stored Parameter Attribute data is corrupt or missing

Refresh Close

Figure 3.6.5:view system event logs

Click “Refresh” to refresh the system event logs or “Close” to exit from this interface.

4.9.3 SNMP Client

4.9.3.1 SNMP Protocol

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

Two versions of SNMP exist: SNMP version 1 (SNMPv1) and SNMP version 2 (SNMPv2). Both versions have a number of features in common, but SNMPv2 offers enhancements, such as additional

protocol operations. Figure 1 illustrates a basic network managed by SNMP.

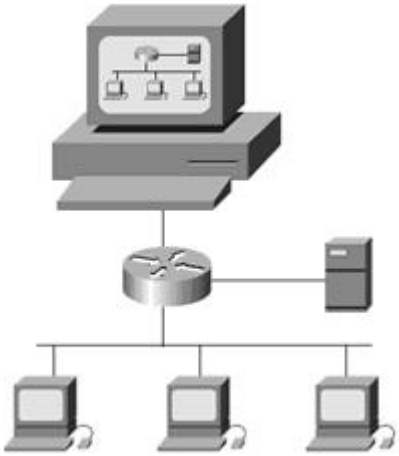


Figure 1 SNMP Facilitates the Exchange of Network Information Between Devices

An SNMP-managed network consists of three key components: managed devices, agents, and network-management systems (NMSs).

A managed device is a network node that contains an SNMP agent and that resides on a managed network. Managed devices collect and store management information and make this information available to NMSs using SNMP. Managed devices, sometimes called network elements, can be routers and access servers, switches and bridges, hubs, computer hosts, or printers.

An agent is a network-management software module that resides in a managed device. An agent has local knowledge of management information and translates that information into a form compatible with SNMP.

An NMS executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs must exist on any managed network.

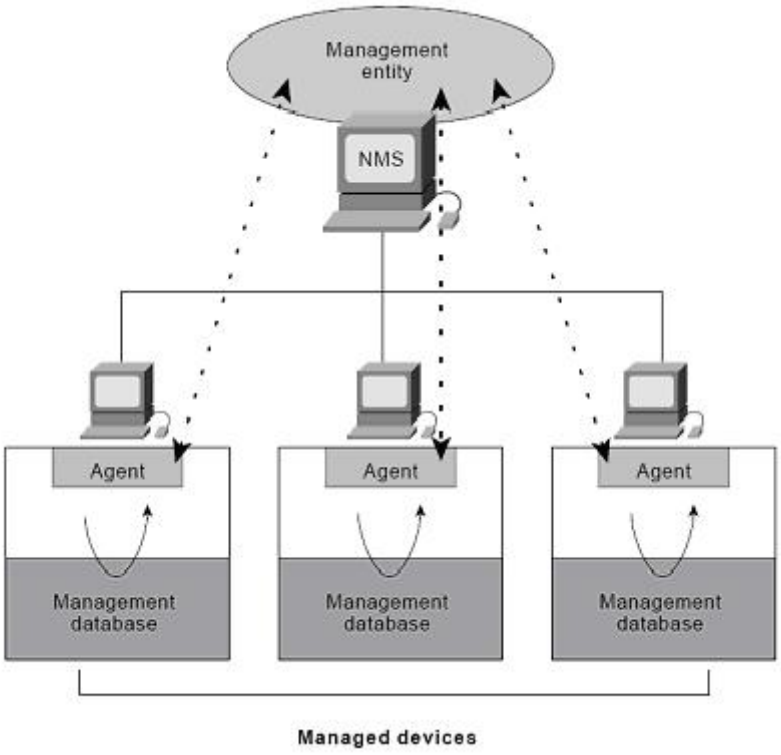


Figure 2 An SNMP-Managed Network Consists of Managed Devices, Agents, and NMSs

Managed devices are monitored and controlled using four basic SNMP commands: read, write, trap, and traversal operations.

The ***read*** command is used by an NMS to monitor managed devices. The NMS examines different variables that are maintained by managed devices.

The ***write*** command is used by an NMS to control managed devices. The NMS changes the values of variables stored within managed devices.

The ***trap*** command is used by managed devices to asynchronously report events to the NMS. When certain types of events occur, a managed device sends a trap to the NMS.

Traversal operations are used by the NMS to determine which variables a managed device supports and to sequentially gather information in variable tables, such as a routing table.

4.9.3.2 Configure

Click “SNMP Agent” sub menu item under “Management” menu item, show figure 3 as following:

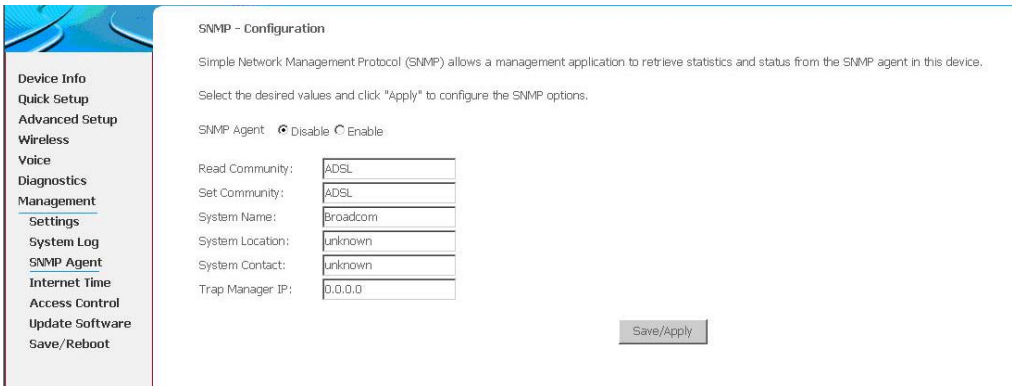


Figure 3.6.6: SNMP Config

Click “Enable” button to open SNMP function, input the configuration that your ISP has provided to you. Then click “Save/Apply”.

4.9.3.3 Simple Test

Use “MIB Browser” tool to test SNMP function, MIB Browser’s main operation interface.

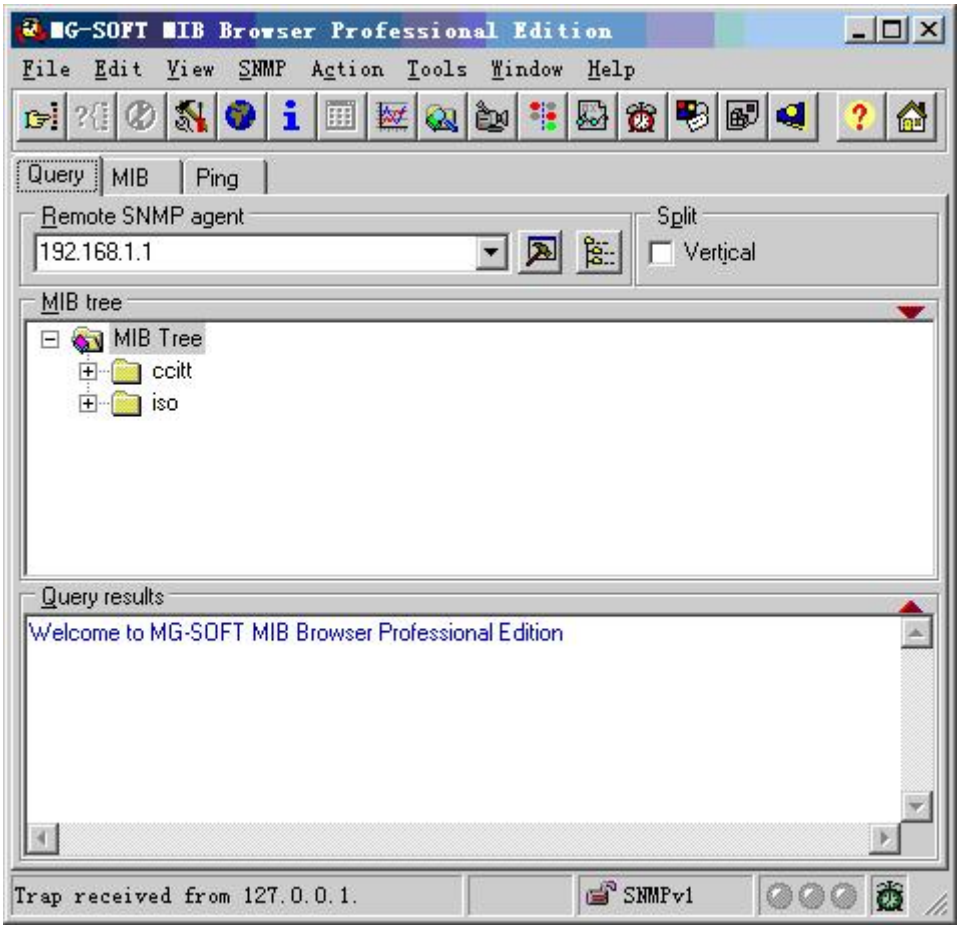


Figure 3.6.7: MIB Browser's main operation interface

Click "view" menu item, then select "SNMP Protocol preferences…" sub menu item, as figure 3:

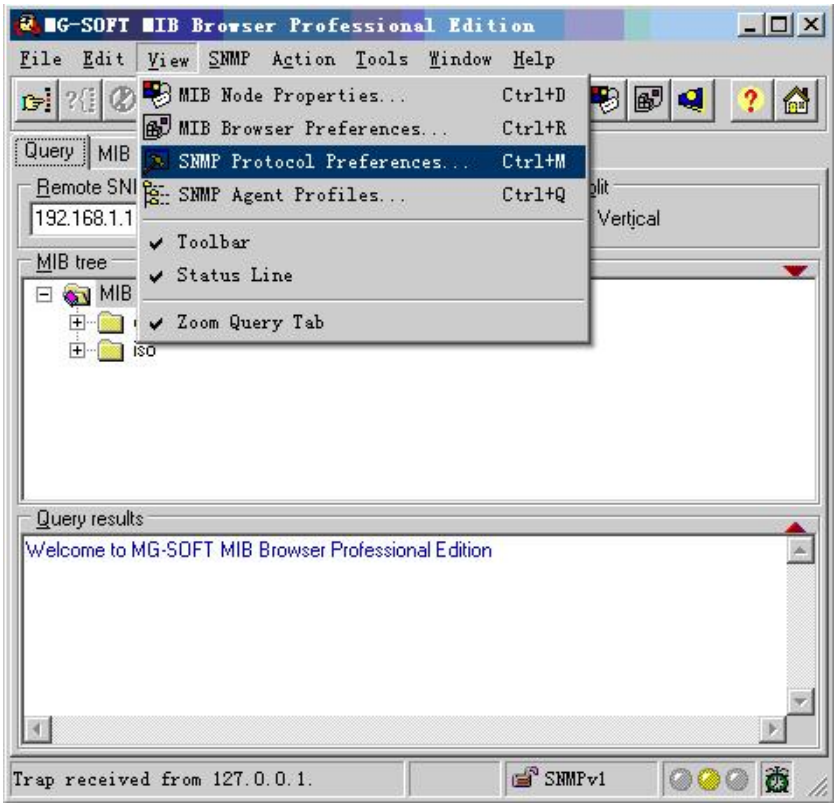


Figure 3.6.7: SNMP Protocol preferences

Show figure 3.6.8 as following:

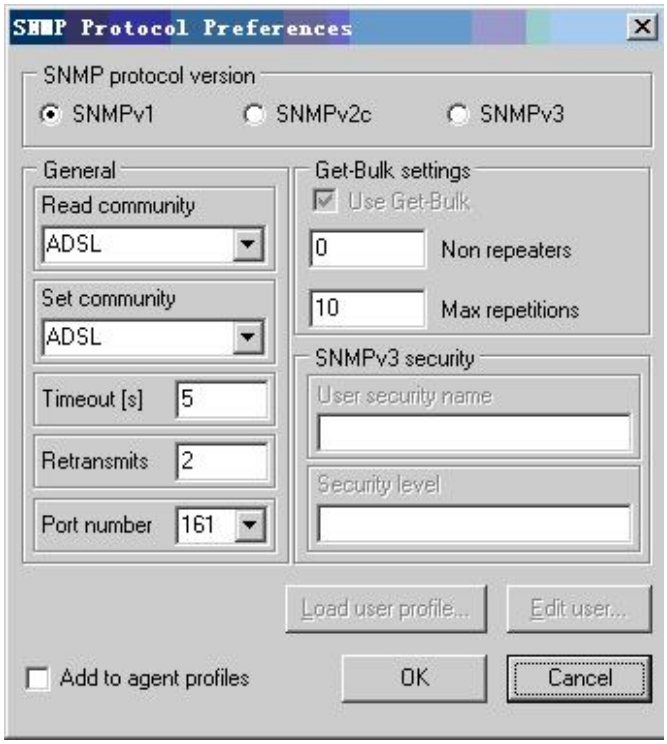


Figure 3.6.8: read community and set community

Select SMP protocol version for SNMPv1, at the read community and set community inputbox, input the string as the same with figure 3.6.8, then click “OK” button.

At “Remote SNMP agent” inputbox input the CPE’s ip address as 192.168.1.1, then click “SNMP” menu item, select the “contact” sub menu item. If connect to CPE successful, in the “Query result” will output the result，as figure 3.6.10

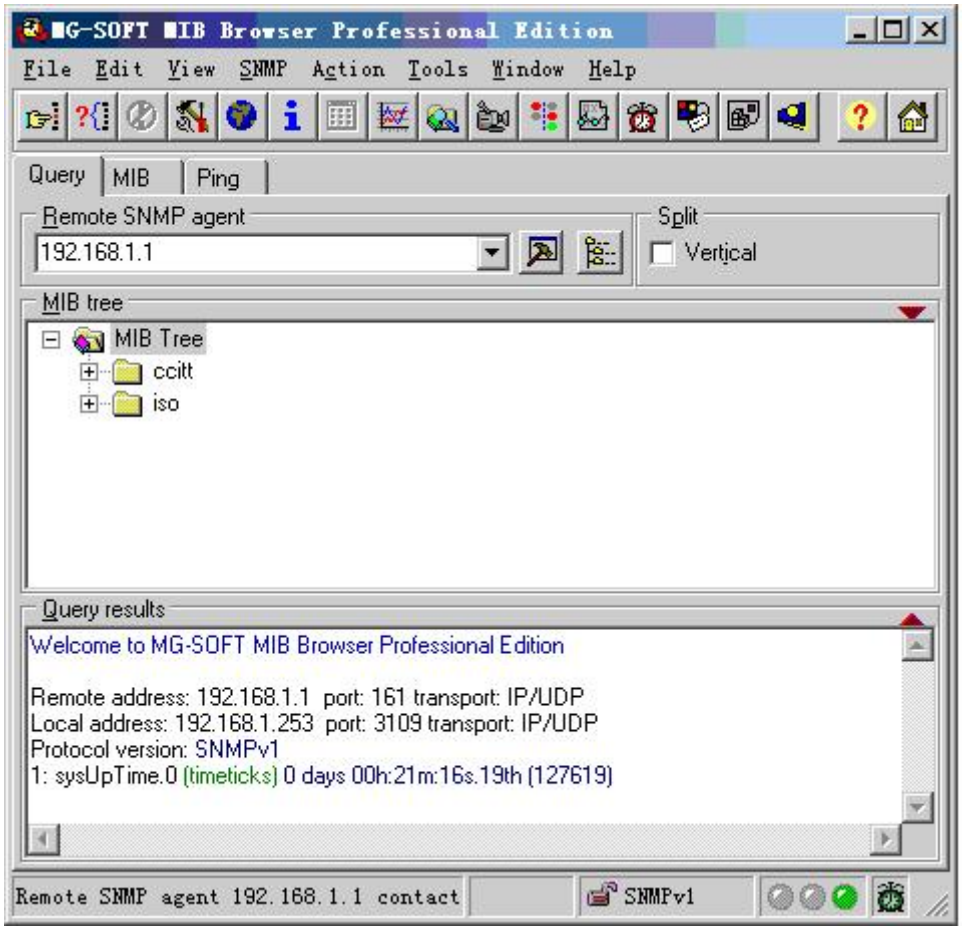


Figure3.6.9:MIB operation

Under “SNMP” menu item, there is “walk” menu item, exec the “walk” operation, if success, in the “Query results” output as figure 3.6.10

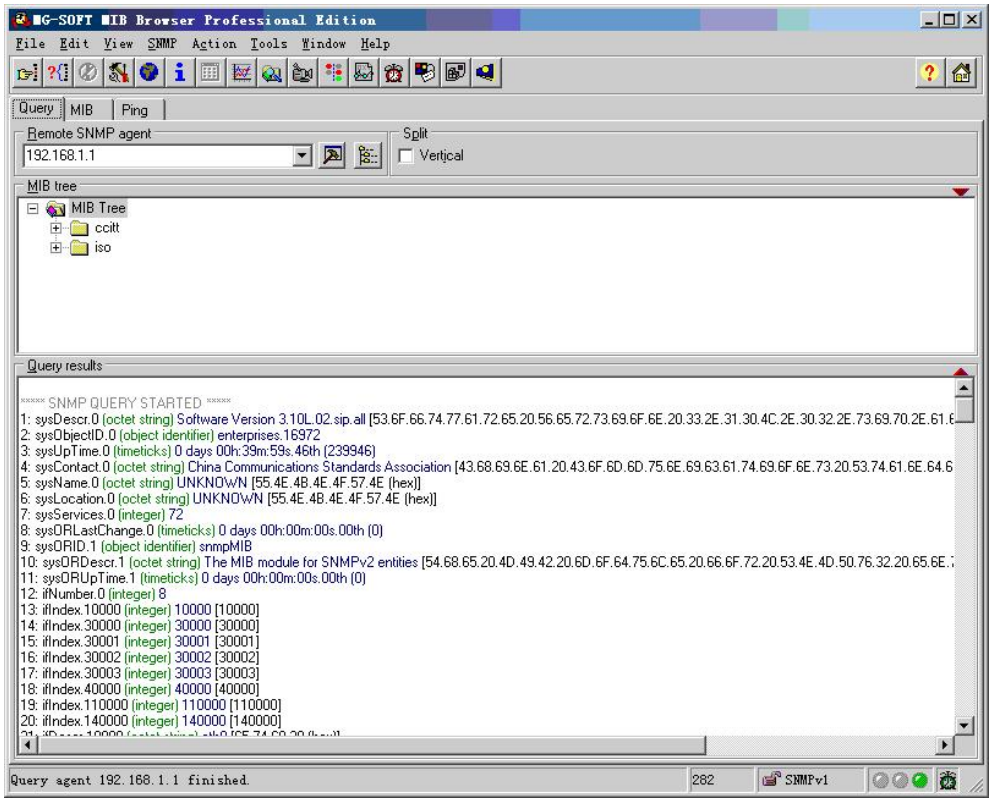

MG-SOFT MIB Browser Professional Edition
File Edit View SNMP Action Tools Window Help
Query MIB Ping
Remote SNMP agent
192.168.1.1
Split
Vertical
MIB tree
MIB Tree
ccitt
iso
Query results
***** SNMP QUERY STARTED *****
1: sysDescr.0 (octet string) Software Version 3.10L.02.sip.all [53.6F.66.74.77.61.72.65.20.56.65.72.73.69.6F.6E.20.33.2E.31.30.4C.2E.30.32.2E.73.69.70.2E.61.6
2: sysObjectID.0 (object identifier) enterprises.16972
3: sysUpTime.0 (timeticks) 0 days 00h:39m:59s.46th (239946)
4: sysContact.0 (octet string) China Communications Standards Association [43.68.69.6E.61.20.43.6F.6D.6D.75.6E.69.63.61.74.69.6F.6E.73.20.53.74.61.6E.64.6
5: sysName.0 (octet string) UNKNOWN [55.4E.4B.4E.4F.57.4E (hex)]
6: sysLocation.0 (octet string) UNKNOWN [55.4E.4B.4E.4F.57.4E (hex)]
7: sysServices.0 (integer) 72
8: sysORLastChange.0 (timeticks) 0 days 00h:00m:00s.00th (0)
9: sysORID.1 (object identifier) snmpMIB
10: sysORDescr.1 (octet string) The MIB module for SNMPv2 entities [54.68.65.20.4D.49.42.20.6D.6F.64.75.6C.65.20.66.6F.72.20.53.4E.4D.50.76.32.20.65.6E.
11: sysORUpTime.1 (timeticks) 0 days 00h:00m:00s.00th (0)
12: ifNumber.0 (integer) 8
13: ifIndex.10000 (integer) 10000 [10000]
14: ifIndex.30000 (integer) 30000 [30000]
15: ifIndex.30001 (integer) 30001 [30001]
16: ifIndex.30002 (integer) 30002 [30002]
17: ifIndex.30003 (integer) 30003 [30003]
18: ifIndex.40000 (integer) 40000 [40000]
19: ifIndex.110000 (integer) 110000 [110000]
20: ifIndex.140000 (integer) 140000 [140000]
Query agent 192.168.1.1 finished.
282
SNMPv1

Figure3.6.10: Query results

4.9.4 TR-69 Client Management

4.9.4.1 Protocol Components

TR-69 is one of the CPE WAN Management Protocol, It comprises several components that are unique to this protocol, and makes use of several standard protocols. The protocol stack defined by the CPE WAN Management Protocol is shown in 错误!未找到引用源。1. A brief description of each layer is provided in Table 1.

CPE/ACS Management Application
RPC Methods
SOAP
HTTP
SSL/TLS
TCP/IP

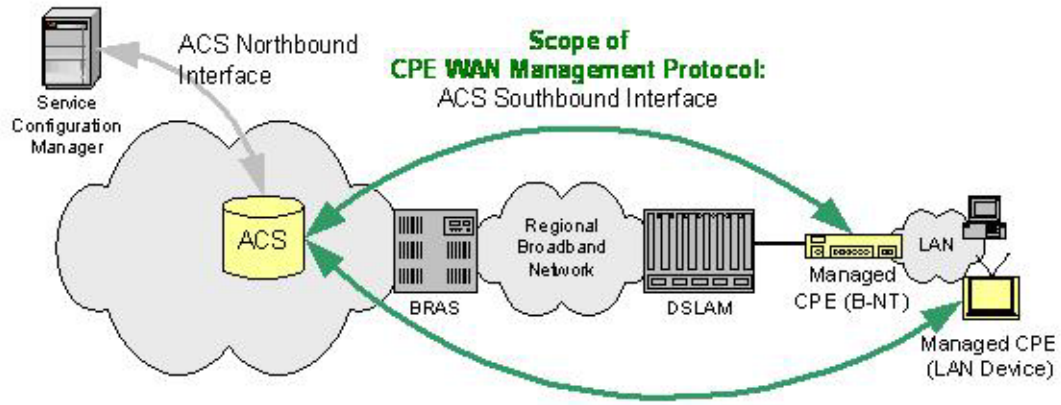
Table 1 – 1 Protocol layer summary

Layer	Description
CPE/ACS Application	The application uses the CPE WAN Management Protocol on the CPE and ACS, respectively. The application is locally defined and not specified as part of the CPE WAN Management Protocol.

Layer	Description
RPC Methods	The specific RPC methods that are defined by the CPE WAN Management Protocol. These methods are specified in 错误！未找到引用源。. This includes the definition of the CPE Parameters accessible by an ACS via the Parameter-related RPC Methods. The specific Parameters defined for an Internet Gateway Device are specified in.
SOAP	A standard XML-based syntax used here to encode remote procedure calls. Specifically SOAP 1.1.
HTTP	HTTP 1.1, as specified in.
SSL/TLS	The standard Internet transport layer security protocols. Specifically, either SSL 3.0 (Secure Socket Layer), as defined in, or TLS 1.0 (Transport Layer Security) as defined in. Use of SSL/TLS is RECOMMENDED but is not required.
TCP/IP	Standard TCP/IP.

4.9.4.2 TR-069 Client-configuration

The CPE WAN Management Protocol is proposed as the protocol to be used on the ACS-Southbound Interface between an Auto-Configuration Server (ACS), this protocol may be used to manage other types of CPE as well, including stand-alone routers and LAN-side client devices, as also shown in 错误！未找到引用源。-2



4.9.4.3 TR-069 Client-configuration

Click “Management” --> “TR-069Client” to show the **TR-069 Client** configuration page.

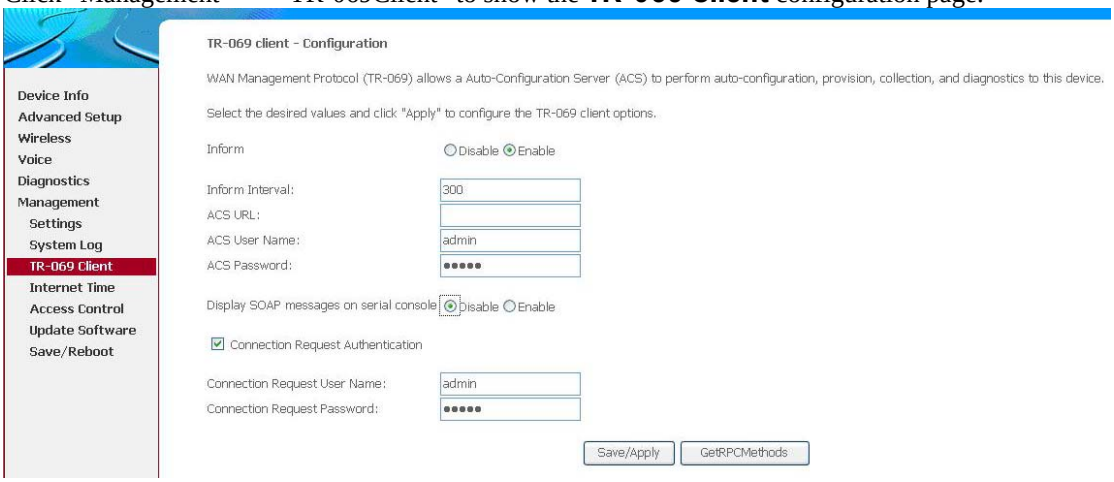


Figure3.7.1:Tr-069 Client –configuration

- Inform：IF the Enable option is selected,the CPE will accept the commands from ACS, the CPE will not accept the commands from ACS when the Disable option is selected.
- Inform Interval: How many seconds does the CPE inform the ACS to connect.
- ACS URL: input the ACS URL
- ACS User Name: The ACS user name is that the TR-069 Service provide to you.
- ACS Password: The ACS password is that the TR-069 Service provide to you.
- Display SOAP messages on serial console: When select Enable option, the SOAP information will display on the serial console, when select disable, it will not.
- Connection Request Authentication**:** If this checkbox is selected, you need to input the Connection Request User Name and the Connection Request Password. or you needn't to input.
- Connection Request User Name: the connection user name that the TR-069 Service provide to you
- Connection Request Password: the Connection Request Password that the TR-069 Service provide to you.
- When Click "Save/Apply", the configuration will save and apply.

4.9.5 Internet Time

Click the "Internet Time", the interface show you. In this page, the MODEM can synchronize with Internet time servers.

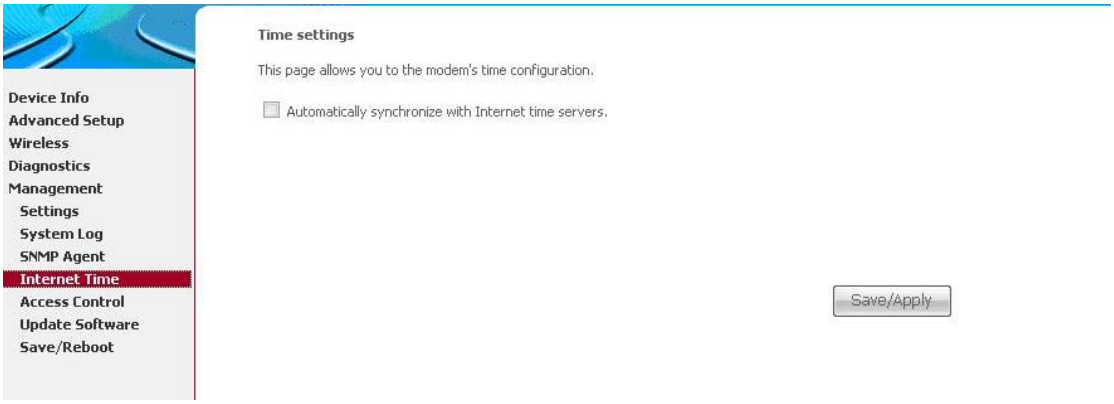


Figure3.7.2: Internet Time overview

After enable "Automatically synchronize with Internet time servers.", the interface show below. Enter proper configurations, then click "Save/Apply".

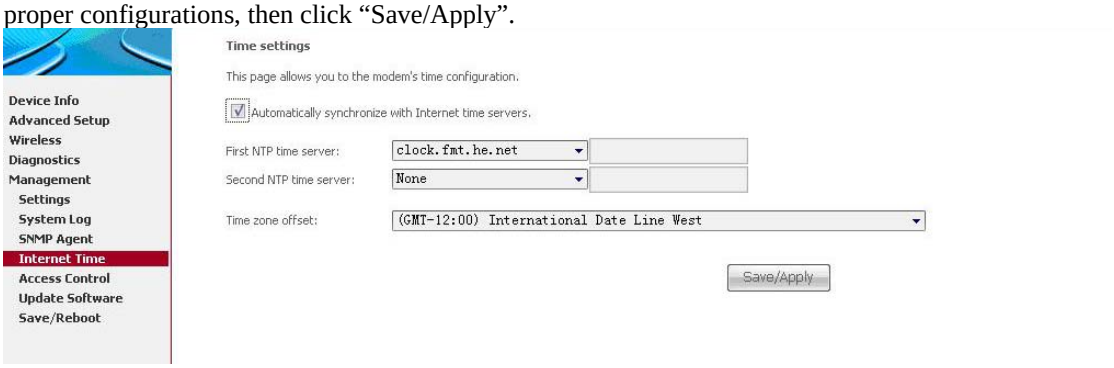


Figure3.7.3:Internet Time Setup

4.9.6 Access Control

4.9.6.1 Access Control – Services

Click "Access Control"-->"Services" to show the following interface. In the interface, you can enable/disable the FTP, HTTP, ICMP, SSH, TELNET and TFTP services. And the LAN side and WAN side can have different configurations.

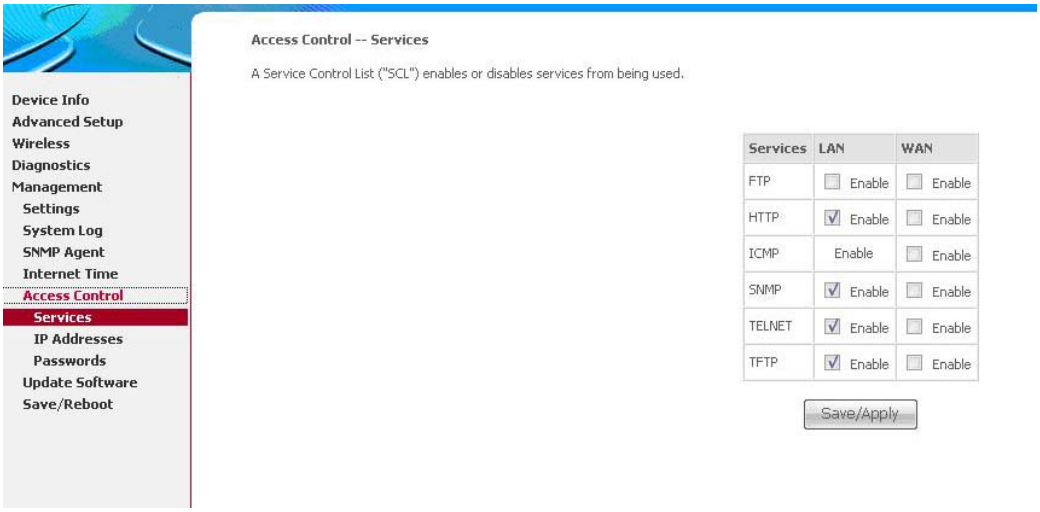


Figure3.7.4:Access Control-Services Setup

4.9.6.2 Access Control -- IP Addresses

Click “Access Control”-->”IP Addresses” to show the following interface.

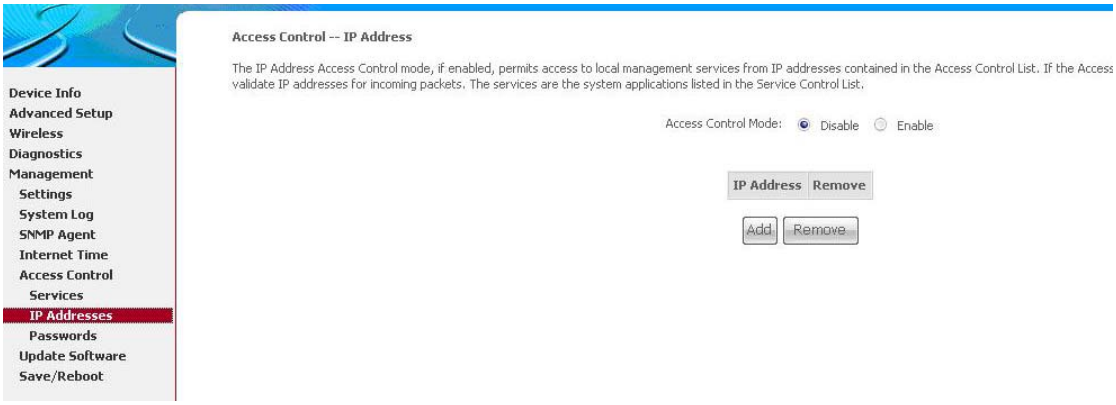


Figure3.7.5:Access Control-IP Addresses overview

If enabled, permits access to local management services from IP addresses contained in the Access Control List.

If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List.

Click “add” to show the following interface. In the interface input the IP address of the management station permitted to access the local management services, and click “Save/Apply”.

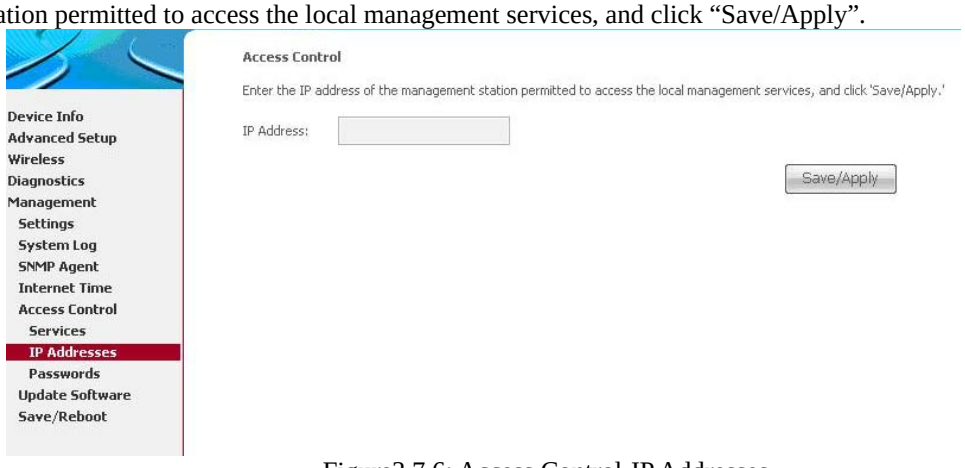


Figure3.7.6: Access Control-IP Addresses

4.9.6.3 Access Control – Passwords

Click “Access Control”-->”Passwords” to show the following interface. In the interface, you can modify the accounts passwords.

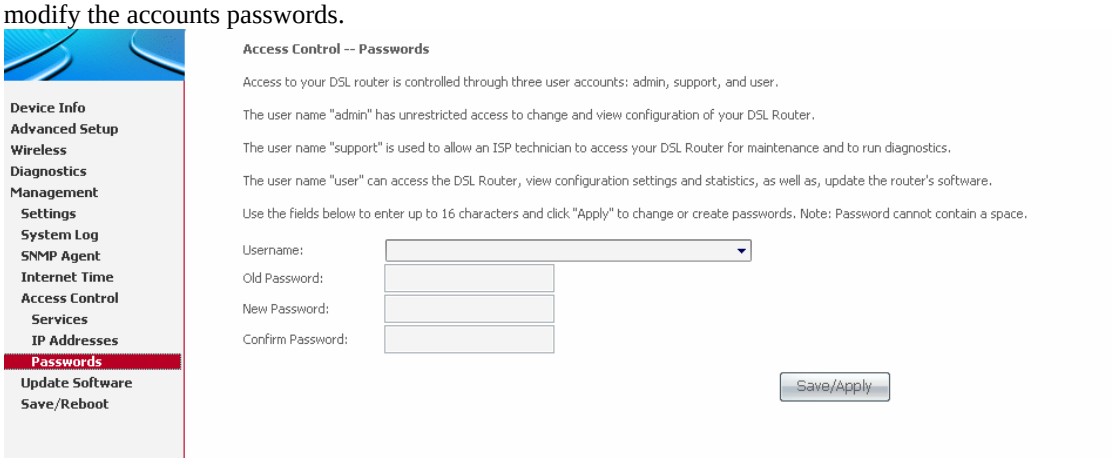

Device Info
Advanced Setup
Wireless
Diagnostics
Management
Settings
System Log
SNMP Agent
Internet Time
Access Control
Services
IP Addresses
Passwords
Update Software
Save/Reboot
Access Control -- Passwords
Access to your DSL router is controlled through three user accounts: admin, support, and user.
The user name "admin" has unrestricted access to change and view configuration of your DSL Router.
The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.
The user name "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's software.
Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cannot contain a space.
Username:
Old Password:
New Password:
Confirm Password:
Save/Apply

Figure3.7.7: Password modify page

4.9.7 Update Software

Click “Update Firmware” to show the following interface. In this interface, you can update the MODEM Firmware. Click the “Browse...” button to find the right version file and press “Update Firmware” to do the update.

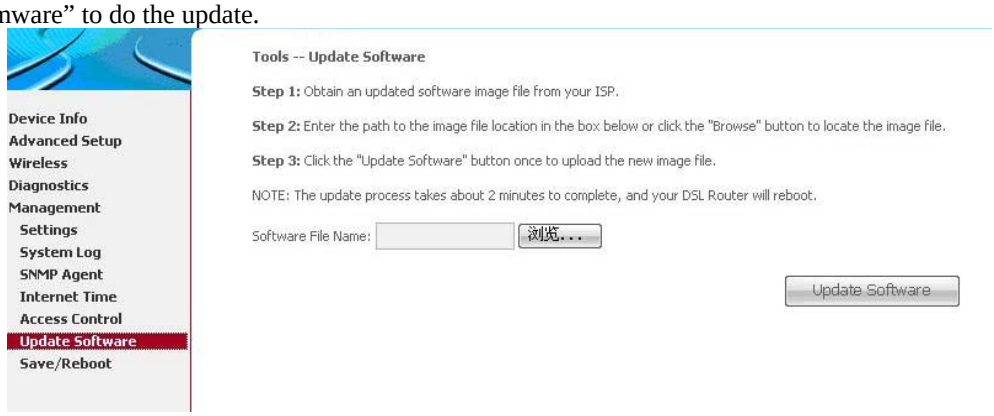

Device Info
Advanced Setup
Wireless
Diagnostics
Management
Settings
System Log
SNMP Agent
Internet Time
Access Control
Update Software
Save/Reboot
Tools -- Update Software
Step 1: Obtain an updated software image file from your ISP.
Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.
Step 3: Click the "Update Software" button once to upload the new image file.
NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.
Software File Name:
浏览...
Update Software

Figure 3.7.8:Update Software page

NOTE: Do not turn off your MODEM during firmware updates. When the update is finished, the MODEM will reboot automatically. Do not turn off your MODEM either before the reboot is over. You must guarantee the update software is right and accurate. It is strictly forbidden to use other software for updates.
After update software, it is suggested to restore the MODEM to the factory defaults and configure it again.

4.9.8 Save/Reboot

Click “Save/Reboot” to show the following interface. Click the “Save/Reboot” button to save and reboot the router.

Figure 3.7.9: Router Save/reboot page